PN - JP2001357373 A 20011226

PD - 2001-12-26

PR - JP20000180054 20000615

OPD - 2000-06-15

TI - DEVICE AND METHOD FOR STORING DATA, DEVICE AND METHOD FOR PROCESSING INFORMATION AND RECORDING MEDIUM

IN - ISHIBASHI YOSHITO;YOSHINO KENJI;ASANO TOMOYUKI;OKA MAKOTO; SHIRAI TAIZO;TAKI RYUTA

PA - SONY CORP

IC - G06K19/073 ; G06K17/00 ; G06K19/10 ; G09C1/00 ; H04L9/10 ; H04L9/32

TI - Data memory device for updating confidential information, controls storage of newer information in memory, after comparison with version of prior information stored in memory

PR - JP20000180054 20000615

PN - JP2001357373 A 20011226 DW200232 G06K19/073 042pp

PA - (SONY) SONY CORP

IC - G06K17/00 ;G06K19/073 ;G06K19/10 ;G09C1/00 ;H04L9/10 ;H04L9/32

AB - JP2001357373 NOVELTY - A comparator compares the version of first confidential information stored in memory with that of second confidential information input by input output controller. When the second information is judged to be newer than the first information, a memory controller controls the memory to store the second information in the storage area of the first information.

- DETAILED DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:
- (a) Data memory method;
- (b) Information processor;
- (c) Information processing method;

- (d) Recorded medium storing data memory program
- USE - For updating confidential information such as authentication key used for interactive authentication with IC card and reader-writer.
- ADVANTAGE - The updating of authentication key stored in the IC card is performed, thereby maintaining the data security using reader-writer.
- DESCRIPTION OF DRAWING(S) - The figure shows the flowchart explaining the authentication process of IC card and reader-writer. (Drawing includes non-English language text).
- (Dwg.15/51)

OPD - 2000-06-15

AN - 2002-275041 [32]

PN - JP2001357373 A 20011226

PD - 2001-12-26

AP - JP20000180054 20000615

IN - OKA MAKOTO;ISHIBASHI YOSHITO;ASANO TOMOYUKI;YOSHINO KENJI;SHIRAI TAIZO;TAKI RYUTA

PA - SONY CORP

TI - DEVICE AND METHOD FOR STORING DATA, DEVICE AND METHOD FOR PROCESSING INFORMATION AND RECORDING MEDIUM

AB - PROBLEM TO BE SOLVED: To update an authentication key which is stored in an IC card through the use of a reader/writer while keeping security.

- SOLUTION: An authentication processing is performed with the IC card in steps S331 and S332, an authentication key ID is enciphered and transmitted in a step S333, a signal from the IC card is received in a step S334, latest version information of the authentication key and the authentication key Kake are enciphered and transmitted in a step S336 when the received signal is an ACK signal, a signal from the IC card is received in a step S337 and a processing is completed when the received signal is the ACK signal. Unless the signal received in the steps S335 and 338 are judged to be the ACK signal, an error message

is displayed in a step S339 and the processing is completed.

- G06K19/073 ;G06K17/00 ;G06K19/10 ;G09C1/00 ;H04L9/10 ;H04L9/32

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－357373
（P2001－357373A）
(43)公開日　平成13年12月26日(2001.12.26)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｋ　19/073		Ｇ０６Ｋ　17/00	Ｅ	５Ｂ０３５
17/00			Ｓ	５Ｂ０５８
		Ｇ０９Ｃ　1/00	６６０Ａ	５Ｊ１０４
19/10		Ｇ０６Ｋ　19/00	Ｐ	
Ｇ０９Ｃ　1/00	６６０		Ｒ	

審査請求　未請求　請求項の数16　ＯＬ　（全 42 頁）　最終頁に続く

(21)出願番号　特願2000－180054(P2000－180054)

(22)出願日　平成12年６月15日(2000.6.15)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　岡　誠
東京都品川区北品川６丁目７番35号　ソニー株式会社内

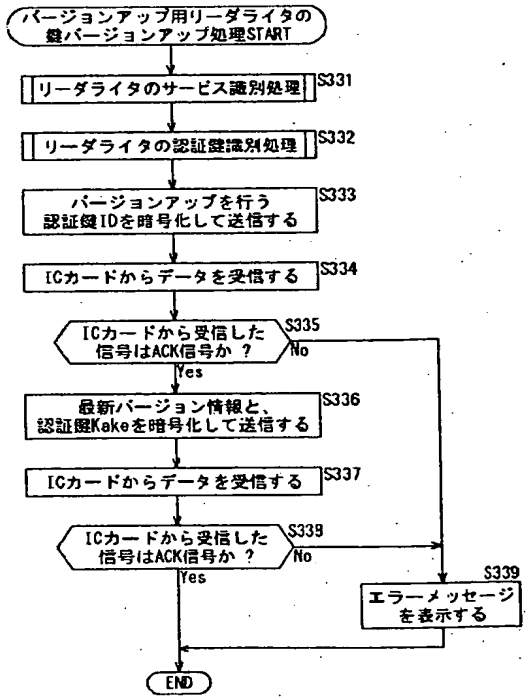
(72)発明者　石橋　義人
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(74)代理人　100082131
弁理士　稲本　義雄

最終頁に続く

(54)【発明の名称】　データ記憶装置およびデータ記憶方法、情報処理装置および情報処理方法、並びに記録媒体

(57)【要約】
【課題】　リーダライタを用いて、セキュリティを維持しつつ、ＩＣカードに記憶されている認証鍵のアップデートを行うことができるようにする。
【解決手段】　ステップＳ３３１およびステップＳ３３２でＩＣカードとの認証処理がなされ、ステップＳ３３３で認証鍵ＩＤが暗号化されて送信され、ステップＳ３３４でＩＣカードからの信号が受信され、受信された信号がＡＣＫ信号であった場合、ステップＳ３３６で認証鍵の最新バージョン情報と認証鍵Kakeが暗号化されて送信され、ステップＳ３３７でＩＣカードからの信号が受信され、受信された信号がＡＣＫ信号であった場合、処理が終了される。ステップＳ３３５およびステップＳ３３８で受信された信号がＡＣＫ信号ではないと判断された場合、ステップＳ３３９でエラーメッセージが表示され、処理が終了される。



【特許請求の範囲】
【請求項１】　情報処理装置に装着され、前記情報処理装置とデータの授受を行うデータ記憶装置において、
前記情報処理装置に対する、前記データの入出力を制御する入出力制御手段と、
秘密情報の記憶を制御する記憶制御手段と、
前記記憶制御手段により記憶が制御された前記秘密情報のうちの第１の秘密情報のバージョン情報と、前記入出力制御手段により入力が制御された第２の秘密情報のバージョン情報より、前記第１の秘密情報のバージョンと、前記第２の秘密情報のバージョンを比較する比較手段とを備え、
前記比較手段により、前記第２の秘密情報のほうが、前記第１の秘密情報よりもバージョンが新しいと判断された場合、前記記憶制御手段は、前記第１の秘密情報を記憶していた記憶領域へ前記第２の秘密情報を記憶させるように制御することを特徴とするデータ記憶装置。
【請求項２】　前記情報処理装置との、前記秘密情報の授受を認証する認証手段を更に備え、
前記認証手段は、前記秘密情報以外の前記データの授受に用いられる第１の認証鍵と異なる第２の認証鍵を用いて、前記秘密情報の授受を認証することを特徴とする請求項１に記載のデータ記憶装置。
【請求項３】　前記入出力制御手段により入力が制御された、暗号化された前記第２の秘密情報を復号する復号手段を更に備え、
前記比較手段により、前記復号手段により復号された前記第２の秘密情報のほうが、前記第１の秘密情報よりもバージョンが新しいと判断された場合、前記記憶制御手段は、前記第１の秘密情報を記憶していた記憶領域へ、前記復号手段により復号された前記第２の秘密情報が記憶されるように制御することを特徴とする請求項１に記載のデータ記憶装置。
【請求項４】　情報処理装置に装着され、前記情報処理装置とデータの授受を行うデータ記憶装置のデータ記憶方法において、
前記情報処理装置に対する、前記データの入出力を制御する入出力制御ステップと、
秘密情報の記憶を制御する記憶制御ステップと、
前記記憶制御ステップの処理により記憶が制御された前記秘密情報のうちの第１の秘密情報のバージョン情報と、前記入出力制御ステップの処理により入力が制御された第２の秘密情報のバージョン情報より、前記第１の秘密情報のバージョンと、前記第２の秘密情報のバージョンを比較する比較ステップとを含み、
前記比較ステップの処理により、前記第２の秘密情報のほうが、前記第１の秘密情報よりもバージョンが新しいと判断された場合、前記記憶制御ステップは、前記第１の秘密情報を記憶していた記憶領域へ前記第２の秘密情報を記憶させるように制御することを特徴とするデータ記憶方法。
【請求項５】　情報処理装置に装着され、前記情報処理装置とデータの授受を行うデータ記憶装置用のプログラムであって、
前記情報処理装置に対する、前記データの入出力を制御する入出力制御ステップと、
秘密情報の記憶を制御する記憶制御ステップと、
前記記憶制御ステップの処理により記憶が制御された前記秘密情報のうちの第１の秘密情報のバージョン情報と、前記入出力制御ステップの処理により入力が制御された第２の秘密情報のバージョン情報より、前記第１の秘密情報のバージョンと、前記第２の秘密情報のバージョンを比較する比較ステップとを含み、
前記比較ステップの処理により、前記第２の秘密情報のほうが、前記第１の秘密情報よりもバージョンが新しいと判断された場合、前記記憶制御ステップは、前記第１の秘密情報を記憶していた記憶領域へ前記第２の秘密情報を記憶させるように制御することを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。
【請求項６】　情報処理装置に装着され、前記情報処理装置とデータの授受を行うデータ記憶装置において、
前記情報処理装置に対する、前記データの入出力を制御する入出力制御手段と、
所定のサービスに対応するデータおよび前記情報処理装置との認証処理に用いられる複数の認証鍵の記憶を制御する記憶制御手段と、
前記記憶制御手段により記憶が制御された複数の前記認証鍵から前記情報処理装置との認証処理に用いられる前記認証鍵を選択する選択手段と、
前記選択手段により選択された前記認証鍵を用いて認証処理を行う認証手段とを備え、
前記選択手段は、選択した第１の認証鍵による認証処理が行えなかった場合、前記第１の認証鍵と異なる第２の認証鍵をさらに選択することを特徴とするデータ記憶装置。
【請求項７】　情報処理装置に装着され、前記情報処理装置とデータの授受を行うデータ記憶装置のデータ記憶方法において、
前記情報処理装置に対する、前記データの入出力を制御する入出力制御ステップと、
所定のサービスに対応するデータおよび前記情報処理装置との認証処理に用いられる複数の認証鍵の記憶を制御する記憶制御ステップと、
前記記憶制御ステップの処理により記憶が制御された複数の前記認証鍵から前記情報処理装置との認証処理に用いられる前記認証鍵を選択する選択ステップと、
前記選択ステップの処理により選択された前記認証鍵を用いて認証処理を行う認証ステップとを含み、
前記選択ステップの処理では、選択された第１の認証鍵

による認証処理が行えなかった場合、前記第１の認証鍵と異なる第２の認証鍵をさらに選択することを特徴とするデータ記憶方法。

【請求項８】　情報処理装置に装着され、前記情報処理装置とデータの授受を行うデータ記憶装置用のプログラムであって、

前記情報処理装置に対する、前記データの入出力を制御する入出力制御ステップと、

所定のサービスに対応するデータおよび前記情報処理装置との認証処理に用いられる複数の認証鍵の記憶を制御する記憶制御ステップと、

前記記憶制御ステップの処理により記憶が制御された複数の前記認証鍵から前記情報処理装置との認証処理に用いられる前記認証鍵を選択する選択ステップと、

前記選択ステップの処理により選択された前記認証鍵を用いて認証処理を行う認証ステップとを含み、

前記選択ステップの処理では、選択された第１の認証鍵による認証処理が行えなかった場合、前記第１の認証鍵と異なる第２の認証鍵をさらに選択することを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項９】　データ記憶装置が装着され、前記データ記憶装置とデータの授受を行う情報処理装置において、

前記データ記憶装置に対する、前記データの入出力を制御する入出力制御手段と、

複数の秘密情報の記憶を制御する記憶制御手段と、

ユーザによる前記秘密情報の選択を示す信号の入力を制御する入力制御手段と、

前記入力制御手段により入力が制御された前記秘密情報の選択を示す信号に基づいて、前記記憶制御手段により記憶が制御された複数の前記秘密情報から所定の前記秘密情報を選択する選択手段とを備え、

前記入出力制御手段は、前記選択手段により選択された前記秘密情報および前記秘密情報のバージョン情報の、前記データ記憶装置への出力を制御することを特徴とする情報処理装置。

【請求項１０】　前記データ記憶装置との、前記秘密情報の授受を認証する認証手段を更に備え、

前記認証手段は、前記秘密情報以外の前記データの授受に用いられる第１の認証鍵と異なる第２の認証鍵を用いて、前記秘密情報の授受を認証することを特徴とする請求項９に記載の情報処理装置。

【請求項１１】　前記選択手段により選択された前記秘密情報を暗号化する暗号化手段を更に備えることを特徴とする請求項９に記載の情報処理装置。

【請求項１２】　データ記憶装置が装着され、前記データ記憶装置とデータの授受を行う情報処理装置の情報処理方法において、

前記データ記憶装置に対する、前記データの入出力を制御する入出力制御ステップと、

複数の秘密情報の記憶を制御する記憶制御ステップと、

ユーザによる前記秘密情報の選択を示す信号の入力を制御する入力制御ステップと、

前記入力制御ステップの処理により入力が制御された前記秘密情報の選択を示す信号に基づいて、前記記憶制御ステップの処理により記憶が制御された複数の前記秘密情報から所定の前記秘密情報を選択する選択ステップとを含み、

前記入出力制御ステップは、前記選択ステップの処理により選択された前記秘密情報および前記秘密情報のバージョン情報の、前記データ記憶装置への出力を制御することを特徴とする情報処理方法。

【請求項１３】　データ記憶装置が装着され、前記データ記憶装置とデータの授受を行う情報処理装置用のプログラムであって、

前記データ記憶装置に対する、前記データの入出力を制御する入出力制御ステップと、

複数の秘密情報の記憶を制御する記憶制御ステップと、

ユーザによる前記秘密情報の選択を示す信号の入力を制御する入力制御ステップと、

前記入力制御ステップの処理により入力が制御された前記秘密情報の選択を示す信号に基づいて、前記記憶制御ステップの処理により記憶が制御された複数の前記秘密情報から所定の前記秘密情報を選択する選択ステップとを含み、

前記入出力制御ステップは、前記選択ステップの処理により選択された前記秘密情報および前記秘密情報のバージョン情報の、前記データ記憶装置への出力を制御することを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項１４】　データ記憶装置が装着され、前記データ記憶装置とデータの授受を行う情報処理装置において、

前記データ記憶装置に対する、前記データの入出力を制御する入出力制御手段と、

所定のサービスに対応するデータおよび前記データ記憶装置との認証処理に用いられる複数の認証鍵の記憶を制御する記憶制御手段と、

前記記憶制御手段により記憶が制御された複数の前記認証鍵から前記データ記憶装置との認証処理に用いられる前記認証鍵を選択する選択手段と、

前記選択手段により選択された前記認証鍵を用いて認証処理を行う認証手段とを備え、

前記記憶制御手段により記憶が制御された複数の前記認証鍵のうち、第１の認証鍵による認証処理が禁止されている場合、前記選択手段は、前記第１の認証鍵と異なる第２の認証鍵を選択することを特徴とする情報処理装置。

【請求項１５】　データ記憶装置が装着され、前記データ記憶装置とデータの授受を行う情報処理装置の情報処

理方法において、
前記データ記憶装置に対する、前記データの入出力を制御する入出力制御ステップと、
所定のサービスに対応するデータおよび前記データ記憶装置との認証処理に用いられる複数の認証鍵の記憶を制御する記憶制御ステップと、
前記記憶制御ステップの処理により記憶が制御された複数の前記認証鍵から前記データ記憶装置との認証処理に用いられる前記認証鍵を選択する選択ステップと、
前記選択ステップの処理により選択された前記認証鍵を用いて認証処理を行う認証ステップとを含み、
前記記憶制御ステップの処理により記憶が制御された複数の前記認証鍵のうち、第1の認証鍵による認証処理が禁止されている場合、前記選択ステップは、前記第1の認証鍵と異なる第2の認証鍵を選択することを特徴とする情報処理方法。
【請求項16】 データ記憶装置が装着され、前記データ記憶装置とデータの授受を行う情報処理装置用のプログラムであって、
前記データ記憶装置に対する、前記データの入出力を制御する入出力制御ステップと、
所定のサービスに対応するデータおよび前記データ記憶装置との認証処理に用いられる複数の認証鍵の記憶を制御する記憶制御ステップと、
前記記憶制御ステップの処理により記憶が制御された複数の前記認証鍵から前記データ記憶装置との認証処理に用いられる前記認証鍵を選択する選択ステップと、
前記選択ステップの処理により選択された前記認証鍵を用いて認証処理を行う認証ステップとを含み、
前記記憶制御ステップの処理により記憶が制御された複数の前記認証鍵のうち、第1の認証鍵による認証処理が禁止されている場合、前記選択ステップは、前記第1の認証鍵と異なる第2の認証鍵を選択することを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は、データ記憶装置およびデータ記憶方法、情報処理装置および情報処理方法、並びに記録媒体に関し、例えば、ICカードとリーダライタとの相互認証に用いられる認証鍵などの、秘密情報のアップデートを、秘密情報アップデート用の認証鍵を用いて、通常のサービスデータの授受とは異なるモードでのICカードとリーダライタ間の通信によって可能としたり、ある認証鍵が第3者に漏洩してしまった場合などに、使用することができなくなった認証鍵以外の他の認証鍵を用いて、認証処理を実行することができるデータ記憶装置およびデータ記憶方法、情報処理装置および情報処理方法、並びに記録媒体に関する。
【0002】
【従来の技術】電子マネーシステムや、セキュリティシステムにおいて、IC（Integrated circuit）カードの利用が増加している。ICカードは、各種処理を行うCPU（Central Processing Unit）や、処理に必要なデータなどを記憶するメモリを内蔵しており、所定のリーダライタに電気的に接触させた状態で、または電磁波を利用して非接触で、データの送受信が行われる。なお、リーダライタとの間で、電磁波を利用して非接触でデータの送受信を行うICカードには、一般に、その電磁波により、必要な電力が供給される。
【0003】ICカードと、リーダライタの認証には、共通鍵方式もしくは公開鍵方式が用いられる。共通鍵方式では、暗号化に使用する鍵と、復号に使用する鍵が同じである，共通鍵暗号を使うには、前もって送信者と受信者の間で共通鍵を共有する必要があるため、暗号化に使用した鍵を、通信路とは別の安全な手段を使って、通信相手に届けておく必要がある（すなわち、ICカードとリーダライタが共通鍵を予め共有していなければならない）。暗号化は、基本的には、文字の順序を入れ換える「転置（転字）」と、一定の規則に従ってある文字を別の文字に置き換える「換字」を組み合わせて行われる。どのような順序で入れ換えるか、どの文字とどの文字が置き換えてあるかを示すのが暗号アルゴリズムと鍵である。暗号化において、文字をずらすための換字暗号や文字の順序を変えるための転置暗号が基本的な暗号変換であり、ずらされる文字数などが鍵となる。
【0004】公開鍵方式は、暗号システムにおいて、「暗号化鍵」と「復号鍵」という2つの鍵をペアで使い、そのうちの暗号化鍵は公開し、復号鍵は、鍵の発行者が管理して秘密にしておくものである。データを送信する場合は、暗号化鍵を使って通信文を暗号化し、受信した側では復号鍵を使って元に戻す。2つの鍵はある数学的な関係に基づいて決められているので、暗号化鍵から復号鍵を求めるのは不可能ではないが、計算量の点から現実的ではない。
【0005】公開鍵暗号システムは、従来の共通鍵暗号システムに比べて、暗号化鍵は秘匿する必要がないので、暗号化鍵の配布が容易であり、暗号文を復号するには、各ユーザが個々に持っている復号鍵さえあればよいので、復号鍵を配布する必要がなく、更に、デジタル署名によるメッセージの認証機能を持つ、という利点を有するが、共通鍵暗号システムに比べて、認証処理にかかる時間が長くなる。
【0006】デジタル署名とは、電子メールやオンライン取り引きなどにおいて、そのメッセージが正当な発信者から発信され、途中で改ざんなどが行なわれていないことを示すための方法である。通常の暗号文通信では、公開鍵で暗号化を行うが、例えば、RSA（Rivest, Shamir, Adleman）公開鍵暗号システムの場合には、逆に、「復号鍵（秘密鍵）で暗号化を行う」とデジタル署

名となる。また、他の暗号方式では、署名を付加したいデータに対して、ハッシュ値を取り、それを秘密鍵で暗号化している。

【0007】この署名を検証するには、公開鍵が用いられる（すなわち、暗号化鍵と復号鍵の役割が入れ換えられる）。公開鍵は広く公開されているので、だれでもその署名の正当性を簡単に検査することができる。もし公開鍵で暗号文を正しく復元することができ、意味のある文が得られれば、それは正しい発信者であると確認することができる。なぜなら、秘密鍵（署名を行った鍵）を知っているのは正規の発信者だけであり、公開鍵で復元できるようなデジタル署名を作成するには、そのペアとなる秘密鍵を知らなければいけないからである。また、データが改ざんされた場合、データは正しく復号することができなくなるため、改ざんの防止・検出にも利用することができる。署名の検証は、公開鍵を用いて復号した値と、別途、データから計算しなおしたハッシュ値とを比較することにより実行され、一致していれば、データは改ざんされていないと判断され、一致していなければ、データの改ざんが行われたと判断される。

【0008】また、データの発行元が信頼のおける組織であることを証明するための証明書を発行することを目的とした第3者の組織を、認証局（CA（Certificate Authority））という。

【0009】

【発明が解決しようとする課題】リーダライタに、ICカード1を装着し、各種サービスを受けるためには、サービス毎に定められた認証鍵を用いて認証処理を行わなければならない。例えば、第3者に、認証鍵が漏洩してしまった場合、これらの認証鍵を用いた認証処理をそのまま継続してしまうと、そのセキュリティが損なわれる恐れがある。また、これらの認証鍵は、セキュリティの維持のために、しばしばバージョンアップされる（すなわち、鍵が変更される）。この場合、従来では、該当するICカードを破棄して、新たなICカードを用いるか、ICカードの発行者が、ICカードに記憶されている認証鍵を書き換える必要があった。

【0010】本発明はこのような状況に鑑みてなされたものであり、ICカードとリーダライタとの相互認証に用いられる認証鍵などの、秘密情報のアップデートを、秘密情報アップデート用の認証鍵を用いて、通常のサービスデータの授受とは異なるモードでのICカードとリーダライタ間の通信によって可能としたり、ある認証鍵が第3者に漏洩してしまった場合などに、使用することができなくなった認証鍵以外の他の認証鍵を用いて、認証処理を実行することを可能とするものである。

【0011】

【課題を解決するための手段】本発明の第1のデータ記憶装置は、情報処理装置に対する、データの入出力を制御する入出力制御手段と、秘密情報の記憶を制御する記憶制御手段と、記憶制御手段により記憶が制御された秘密情報のうちの第1の秘密情報のバージョン情報と、入出力制御手段により入力が制御された第2の秘密情報のバージョン情報より、第1の秘密情報のバージョンと、第2の秘密情報のバージョンを比較する比較手段とを備え、比較手段により、第2の秘密情報のほうが、第1の秘密情報よりもバージョンが新しいと判断された場合、記憶制御手段は、第1の秘密情報を記憶していた記憶領域へ第2の秘密情報を記憶させるように制御することを特徴とする。

【0012】情報処理装置との、秘密情報の授受を認証する認証手段を更に備えることができ、認証手段には、秘密情報以外のデータの授受に用いられる第1の認証鍵と異なる第2の認証鍵を用いて、秘密情報の授受を認証させることができる。

【0013】入出力制御手段により入力が制御された、暗号化された第2の秘密情報を復号する復号手段を更に備えることができ、比較手段により、復号手段により復号された第2の秘密情報のほうが、第1の秘密情報よりもバージョンが新しいと判断された場合、記憶制御手段には、第1の秘密情報を記憶していた記憶領域へ、復号手段により復号された第2の秘密情報が記憶されるように制御させることができる。

【0014】本発明の第1のデータ記憶方法は、情報処理装置に対する、データの入出力を制御する入出力制御ステップと、秘密情報の記憶を制御する記憶制御ステップと、記憶制御ステップの処理により記憶が制御された秘密情報のうちの第1の秘密情報のバージョン情報と、入出力制御ステップの処理により入力が制御された第2の秘密情報のバージョン情報より、第1の秘密情報のバージョンと、第2の秘密情報のバージョンを比較する比較ステップとを含み、比較ステップの処理により、第2の秘密情報のほうが、第1の秘密情報よりもバージョンが新しいと判断された場合、記憶制御ステップは、第1の秘密情報を記憶していた記憶領域へ第2の秘密情報を記憶させるように制御することを特徴とする。

【0015】本発明の第1の記録媒体に記録されているプログラムは、情報処理装置に対する、データの入出力を制御する入出力制御ステップと、秘密情報の記憶を制御する記憶制御ステップと、記憶制御ステップの処理により記憶が制御された秘密情報のうちの第1の秘密情報のバージョン情報と、入出力制御ステップの処理により入力が制御された第2の秘密情報のバージョン情報より、第1の秘密情報のバージョンと、第2の秘密情報のバージョンを比較する比較ステップとを含み、比較ステップの処理により、第2の秘密情報のほうが、第1の秘密情報よりもバージョンが新しいと判断された場合、記憶制御ステップは、第1の秘密情報を記憶していた記憶領域へ第2の秘密情報を記憶させるように制御することを特徴とする。

【００１６】本発明の第２のデータ記憶装置は、情報処理装置に対する、データの入出力を制御する入出力制御手段と、所定のサービスに対応するデータおよび情報処理装置との認証処理に用いられる複数の認証鍵の記憶を制御する記憶制御手段と、記憶制御手段により記憶が制御された複数の認証鍵から情報処理装置との認証処理に用いられる認証鍵を選択する選択手段と、選択手段により選択された認証鍵を用いて認証処理を行う認証手段とを備え、選択手段は、選択した第１の認証鍵による認証処理が行えなかった場合、第１の認証鍵と異なる第２の認証鍵をさらに選択することを特徴とする。

【００１７】本発明の第２のデータ記憶方法は、情報処理装置に対する、データの入出力を制御する入出力制御ステップと、所定のサービスに対応するデータおよび情報処理装置との認証処理に用いられる複数の認証鍵の記憶を制御する記憶制御ステップと、記憶制御ステップの処理により記憶が制御された複数の認証鍵から情報処理装置との認証処理に用いられる認証鍵を選択する選択ステップと、選択ステップの処理により選択された認証鍵を用いて認証処理を行う認証ステップとを含み、選択ステップの処理では、選択された第１の認証鍵による認証処理が行えなかった場合、第１の認証鍵と異なる第２の認証鍵をさらに選択することを特徴とする。

【００１８】本発明の第２の記録媒体に記録されているプログラムは、情報処理装置に対する、データの入出力を制御する入出力制御ステップと、所定のサービスに対応するデータおよび情報処理装置との認証処理に用いられる複数の認証鍵の記憶を制御する記憶制御ステップと、記憶制御ステップの処理により記憶が制御された複数の認証鍵から情報処理装置との認証処理に用いられる認証鍵を選択する選択ステップと、選択ステップの処理により選択された認証鍵を用いて認証処理を行う認証ステップとを含み、選択ステップでは、選択された第１の認証鍵による認証処理が行えなかった場合、第１の認証鍵と異なる第２の認証鍵をさらに選択することを特徴とする。

【００１９】本発明の第１の情報処理装置は、データ記憶装置に対する、データの入出力を制御する入出力制御手段と、複数の秘密情報の記憶を制御する記憶制御手段と、ユーザによる秘密情報の選択を示す信号の入力を制御する入力制御手段と、入力制御手段により入力が制御された秘密情報の選択を示す信号に基づいて、記憶制御手段により記憶が制御された複数の秘密情報から所定の秘密情報を選択する選択手段とを備え、入出力制御手段は、選択手段により選択された秘密情報および秘密情報のバージョン情報の、データ記憶装置への出力を制御することを特徴とする。

【００２０】データ記憶装置との、秘密情報の授受を認証する認証手段を更に備えることができ、認証手段には、秘密情報以外のデータの授受に用いられる第１の認証鍵と異なる第２の認証鍵を用いて、秘密情報の授受を認証させることができる。

【００２１】選択手段により選択された秘密情報を暗号化する暗号化手段を更に備えることができる。

【００２２】本発明の第１の情報処理方法は、データ記憶装置に対する、データの入出力を制御する入出力制御ステップと、複数の秘密情報の記憶を制御する記憶制御ステップと、ユーザによる秘密情報の選択を示す信号の入力を制御する入力制御ステップと、入力制御ステップの処理により入力が制御された秘密情報の選択を示す信号に基づいて、記憶制御ステップの処理により記憶が制御された複数の秘密情報から所定の秘密情報を選択する選択ステップとを含み、入出力制御ステップは、選択ステップの処理により選択された秘密情報および秘密情報のバージョン情報の、データ記憶装置への出力を制御することを特徴とする。

【００２３】本発明の第１の記録媒体に記録されているプログラムは、データ記憶装置に対する、データの入出力を制御する入出力制御ステップと、複数の秘密情報の記憶を制御する記憶制御ステップと、ユーザによる秘密情報の選択を示す信号の入力を制御する入力制御ステップと、入力制御ステップの処理により入力が制御された秘密情報の選択を示す信号に基づいて、記憶制御ステップの処理により記憶が制御された複数の秘密情報から所定の秘密情報を選択する選択ステップとを含み、入出力制御ステップは、選択ステップの処理により選択された秘密情報および秘密情報のバージョン情報の、データ記憶装置への出力を制御することを特徴とする。

【００２４】本発明の第２の情報処理装置は、データ記憶装置に対する、データの入出力を制御する入出力制御手段と、所定のサービスに対応するデータおよびデータ記憶装置との認証処理に用いられる複数の認証鍵の記憶を制御する記憶制御手段と、記憶制御手段により記憶が制御された複数の認証鍵からデータ記憶装置との認証処理に用いられる認証鍵を選択する選択手段と、選択手段により選択された認証鍵を用いて認証処理を行う認証手段とを備え、記憶制御手段により記憶が制御された複数の認証鍵のうち、第１の認証鍵による認証処理が禁止されている場合、選択手段は、第１の認証鍵と異なる第２の認証鍵を選択することを特徴とする。

【００２５】本発明の第２の情報処理方法は、データ記憶装置に対する、データの入出力を制御する入出力制御ステップと、所定のサービスに対応するデータおよびデータ記憶装置との認証処理に用いられる複数の認証鍵の記憶を制御する記憶制御ステップと、記憶制御ステップの処理により記憶が制御された複数の認証鍵からデータ記憶装置との認証処理に用いられる認証鍵を選択する選択ステップと、選択ステップの処理により選択された認証鍵を用いて認証処理を行う認証ステップとを含み、記憶制御ステップの処理により記憶が制御された複数の認

証鍵のうち、第1の認証鍵による認証処理が禁止されている場合、選択ステップは、第1の認証鍵と異なる第2の認証鍵を選択することを特徴とする。

【００２６】本発明の第2の記録媒体に記録されているプログラムは、データ記憶装置に対する、データの入出力を制御する入出力制御ステップと、所定のサービスに対応するデータおよびデータ記憶装置との認証処理に用いられる複数の認証鍵の記憶を制御する記憶制御ステップと、記憶制御ステップの処理により記憶が制御された複数の認証鍵からデータ記憶装置との認証処理に用いられる認証鍵を選択する選択ステップと、選択ステップの処理により選択された認証鍵を用いて認証処理を行う認証ステップとを含み、記憶制御ステップの処理により記憶が制御された複数の認証鍵のうち、第1の認証鍵による認証処理が禁止されている場合、選択ステップは、第1の認証鍵と異なる第2の認証鍵を選択することを特徴とする。

【００２７】本発明の第1のデータ記憶装置、データ記憶方法、および記録媒体に記録されているプログラムにおいては、情報処理装置に対する、データの入出力が制御され、秘密情報の記憶が制御され、記憶された秘密情報のうちの第1の秘密情報のバージョン情報と、入力された第2の秘密情報のバージョン情報より、第1の秘密情報のバージョンと、第2の秘密情報のバージョンが比較され、第2の秘密情報のほうが、第1の秘密情報よりもバージョンが新しいと判断された場合、第1の秘密情報を記憶していた記憶領域へ第2の秘密情報を記憶させるように制御される。

【００２８】本発明の第2のデータ記憶装置、データ記憶方法、および記録媒体に記録されているプログラムにおいては、情報処理装置に対する、データの入出力が制御され、所定のサービスに対応するデータおよび情報処理装置との認証処理に用いられる複数の認証鍵の記憶が制御され、記憶された複数の認証鍵から情報処理装置との認証処理に用いられる認証鍵が選択され、選択された認証鍵を用いて認証処理が行われ、選択された第1の認証鍵による認証処理が行えなかった場合、第1の認証鍵と異なる第2の認証鍵がさらに選択される。

【００２９】本発明の第1の情報処理装置、情報処理方法、および記録媒体に記録されているプログラムにおいては、データ記憶装置に対する、データの入出力が制御され、複数の秘密情報の記憶が制御され、ユーザによる秘密情報の選択を示す信号の入力が制御され、入力された秘密情報の選択を示す信号に基づいて、記憶された複数の秘密情報から所定の秘密情報が選択され、選択された秘密情報および秘密情報のバージョン情報の、データ記憶装置への出力が制御される。

【００３０】本発明の第2の情報処理装置、情報処理方法、および記録媒体に記録されているプログラムにおいては、データ記憶装置に対する、データの入出力が制御され、所定のサービスに対応するデータおよびデータ記憶装置との認証処理に用いられる複数の認証鍵の記憶が制御され、記憶された複数の認証鍵からデータ記憶装置との認証処理に用いられる認証鍵が選択され、選択された認証鍵を用いて認証処理が行われ、記憶されている複数の認証鍵のうち、第1の認証鍵による認証処理が禁止されている場合、第1の認証鍵と異なる第2の認証鍵が選択される。

【００３１】

【発明の実施の形態】以下、図を参照して、本発明の実施の形態について説明する。

【００３２】図1に、ＩＣカードとリーダライタの関係を示す。ＩＣカード1は、共通鍵方式による認証と、公開鍵方式による認証の両方の認証サービスに対応することが可能である（それぞれの認証方法については後述する）。非接触式共通鍵対応リーダライタ２－１は、ＩＣカード1と非接触で通信を行い、共通鍵方式で認証を行う。非接触式公開鍵対応リーダライタ２－２は、ＩＣカード1と非接触で通信を行い、公開鍵方式で認証を行う。接触式公開鍵対応リーダライタ２－３は、接触して通信を行い、公開鍵方式で通信を行う。

【００３３】例えば、ＩＣカード1に定期券や運賃の支払いを行うことができるプリペイドカードなどのサービスを提供する情報が含まれており、ＩＣカード1を用いて駅の改札を利用する場合や、ＩＣカード1に、ＩＤカードとしての機能が含まれており、ＩＣカード1を用いて入室許可の認証を行う場合などの、短い処理時間が求められる処理においては、非接触式共通鍵対応リーダライタ２－１を用いて、共通鍵による非接触の通信が行われる。

【００３４】例えば、ＩＣカード1に、電子マネーのサービスを提供する情報が含まれており、店舗などでユーザが購買した商品の清算の処理を行う場合などは、公開鍵方式により認証が行われ、認証処理に時間がかかる。このため、処理時間を特に気にしないような場合は、非接触式公開鍵対応リーダライタ２－２を用いて、非接触で通信を行ってもよいし、処理時間を短縮するために、接触式公開鍵対応リーダライタ２－３を用いて、接触して通信を行うようにしてもよい。

【００３５】図1においては、非接触式共通鍵対応リーダライタ２－１乃至接触式公開鍵対応リーダライタ２－３を、個別のリーダライタとして説明しているが、必要に応じて、１つのリーダライタで、複数の通信方法や複数の認証方法を用いることができるようにしてもよい。

【００３６】次に、図2を用いて、カード発行者、サービス提供者、およびカード保持者について説明する。

【００３７】カード発行者１１は、サービス提供者１２に、ＩＣカード1を保有するカード保持者１３に対して、ＩＣカード1を用いたサービスの提供を行うことを認可し、ＩＣカード1の発行を希望したカード保持者1

3に対して、ＩＣカード１を発行する。

【００３８】カード発行者１１から、サービスの認可を受けたサービス提供者１２は、カード発行者１１が有するサービス登録用リーダライタ２－１１に、自分自身がカード保持者１３に提供するサービスに対応するデータ（図６を用いて後述するService Individual Info）を登録する。この登録については、例えば、サービス提供者１２が有する図示しないパーソナルコンピュータなどから、インターネットなどを介して、サービス登録用リーダライタ２－１１に登録するようにしてもよいし、オペレータが手動で登録するようにしてもよい。

【００３９】カード保持者１３は、サービス登録用リーダライタ２－１１を用いて、カード発行者１１から発行されたＩＣカード１に、希望するサービスを登録させることができる。サービス登録用リーダライタ２－１１と、ＩＣカード１のサービス登録処理については、図２９および図３０を用いて後述する。

【００４０】そして、カード保持者１３は、自分自身のＩＣカード１に登録されているサービスの削除を行いたい場合、カード発行者１１が管理するサービス登録用リーダライタ２－１１、もしくは、サービス提供者１２が管理する一般リーダライタ２－１２を用いて、自分自身のＩＣカード１から、サービスを削除させることができる。ＩＣカード１とサービス登録用リーダライタ２－１１のサービス削除処理については、図３１および図３２、ＩＣカード１と一般リーダライタ２－１２のサービス削除処理については、図３３および図３４を用いて後述する。

【００４１】また、カード保持者１３は、例えば、ＩＣカード１に、電子マネーサービスとプリペイドサービスが登録されており、それぞれの価値情報が、ＩＣカード１のそれぞれのサービスに関する情報に記録されている状況で、電子マネーの価値の一部を、プリペイドの価値へ置き換えたい場合、サービス提供者１２が管理するモジュール間通信用リーダライタ２－１３を用いて、自分自身のＩＣカード１の、図１３を用いて後述する公開鍵モジュールと共通鍵モジュールの間で、モジュール間通信を実行させることができる。モジュール間通信用リーダライタ２－１３は、共通鍵方式と、公開鍵方式の２方式に対応するようになされている。ＩＣカード１とモジュール間通信用リーダライタ２－１３との処理については、図４８乃至図５１を用いて後述する。

【００４２】更に、カード保持者１３は、失効してしまった認証鍵の更新（バージョンアップ）を行いたい場合、サービス提供者１２が管理する一般リーダライタ２－１２、もしくは、バージョンアップ用リーダライタ２－１４を用いて、自分自身のＩＣカード１に登録されている認証鍵のバージョンアップを行わせることができる。ＩＣカード１とバージョンアップ用リーダライタ２－１４との鍵バージョンアップ処理については、図４３および４４を用いて、ＩＣカード１と一般リーダライタ２－１２との鍵バージョンアップ処理については、図４５乃至４７を用いて後述する。

【００４３】図３は、ＩＣカード１の構成を示すブロック図である。

【００４４】ＩＣカード１は、リーダライタ２（リーダライタ２－１乃至２－３、もしくはリーダライタ２－１１乃至２－１４を特に区別する必要のない場合については、これらを総称して、リーダライタ２と称するものとする）との通信を行う通信部２１と、データ処理を実行するＩＣカード処理部２２から構成されている。

【００４５】通信部２１は、対応するＩＣカード１が、図１を用いて説明した非接触式共通鍵対応リーダライタ２－１、もしくは非接触式公開鍵対応リーダライタ２－２である場合、非接触式共通鍵対応リーダライタ２－１、もしくは非接触式公開鍵対応リーダライタ２－２と、電磁波を用いて通信するためのコイルを備えている。また、通信部２１は、ＩＣカード１が、図１を用いて説明した非接触式共通鍵対応リーダライタ２－１、および非接触式公開鍵対応リーダライタ２－２のみならず、接触式公開鍵対応リーダライタ２－３との通信にも対応している場合、非接触式共通鍵対応リーダライタ２－１、もしくは非接触式公開鍵対応リーダライタ２－２と、電磁波を用いて通信するためのコイルと、接触式公開鍵対応リーダライタ２－３と通信するための接触端子を備えている。

【００４６】通信部２１は、リーダライタ２から送信されたデータを受信し、受信したデータが、例えば、ＡＳＫ（Amplitude Shift Keying）やＢＰＳＫ（Binary Phase Shift Keying）を用いて変調されている場合、所定の処理により、受信したデータを復調し、ＩＣカード処理部２２の制御部３１に供給するとともに、ＩＣカード処理部２２の処理により生成されたデータを、制御部３１から供給され、ＡＳＫやＢＰＳＫを用いて変調し、リーダライタ２に送信する。

【００４７】ＩＣカード処理部２２は、制御部３１、メモリ３２、および暗号処理部３３より構成されている。制御部３１は、通信部２１から供給されたデータに従って、暗号処理部３３を制御し、リーダライタ２との認証処理等に必要な暗号処理を実行させたり、必要に応じて、メモリ３２に記録されているデータを読み込んで、通信部２１を介して、リーダライタ２に送信する。

【００４８】メモリ３２は、カードＩＤ、サービス登録用の認証鍵Kreg、認証局の公開鍵であるCA_Pubが記録されているメモリ領域４４、図８を用いて後述するService Relation Table（ＳＲＴ）４５、および図６を用いて後述するService Registration Area（ＳＲＡ）４６で構成されている。

【００４９】暗号処理部３３は、公開鍵処理部４１、共通鍵処理部４２、その他の暗号処理部４３で構成されて

いる。公開鍵処理部４１乃至その他の暗号処理部４３が実行する処理に関する詳細は、図５を用いて後述する。

【００５０】次に、図４は、ＩＣカード１の、図３と異なる構成を示すブロック図である。なお、図４のＩＣカード１においては、図３における場合と対応する部分には同一の符号を付してあり、その説明は適宜省略する（以下、同様）。

【００５１】ＩＣカード１は、共通鍵サービスに関するリーダライタ２との通信を実行する通信部５１、通信部５１の処理によって得られたデータの処理を実行する共通鍵サービス処理部５２、公開鍵サービスに関するリーダライタ２との通信を実行する通信部５３、通信部５３の処理によって得られたデータの処理を実行する公開鍵サービス処理部５４から構成されている。

【００５２】通信部５１は、非接触式共通鍵対応リーダライタ２－１と通信を行うためのコイルを備えており、通信部２１と同様に、例えば、ＩＣカード1から送信されるデータが、ＡＳＫやＢＰＳＫを用いて変調されている場合、所定の処理により、受信したデータを復調し、共通鍵サービス処理部５２の制御部６１に供給するとともに、共通鍵サービス処理部５２の処理により生成されたデータを、制御部６１から供給され、ＡＳＫやＢＰＳＫを用いて変調し、リーダライタ２に送信する。

【００５３】共通鍵サービス処理部５２は、制御部６１、メモリ６２、および暗号処理部６３から構成されている。制御部６１は、通信部５１から供給されたデータに従って、暗号処理部６３を制御し、ＩＣカード１との認証処理等に必要な処理を実行させたり、必要に応じて、メモリ６２に記録されているデータを読み込んで、通信部５１を介して、リーダライタ２に送信する。

【００５４】メモリ６２は、図３を用いて説明したメモリ３２と同様に、メモリ領域４４、ＳＲＴ４５、およびＳＲＡ４６で構成されている。メモリ領域４４には、カードＩＤ、サービス登録用の認証鍵Kres、および、モジュール間通信で用いられる共有秘密鍵K_commonが記録されている。

【００５５】暗号処理部６３は、共通鍵処理部４２、その他の暗号処理部４３で構成されている。すなわち、共通鍵サービス処理部５２においては、公開鍵に関するサービスを処理しないため、暗号処理部６３には、図３を用いて説明した公開鍵処理部４１は備えられていない。

【００５６】通信部５３は、非接触式公開鍵対応リーダライタ２－２、あるいは、接触式公開鍵対応リーダライタ２－３と通信を行うためのコイルもしくは接触端子を備えている。通信部５３も、通信部２１と同様に、例えば、ＩＣカード1から送信されるデータが、ＡＳＫやＢＰＳＫを用いて変調されている場合、所定の処理により、受信したデータを復調し、公開鍵サービス処理部５４の制御部６１に供給するとともに、公開鍵サービス処理部５４の処理により生成されたデータを、制御部６１から供給され、ＡＳＫやＢＰＳＫを用いて変調し、リーダライタ２に送信する。

【００５７】公開鍵サービス処理部５４は、制御部６１、メモリ６２、および暗号処理部３３から構成されている。すなわち、暗号処理部６３に代わって、図３を用いて説明した暗号処理部３３が備えられている以外は、共通鍵サービス処理部と、基本的に同様の構成である。

【００５８】次に、図５を用いて、公開鍵処理部４１乃至その他の暗号処理部４３について説明する。

【００５９】図５（Ａ）に示されるように、公開鍵処理部４１には、例えば、ＲＳＡ（Rivest, Shamir, Adleman）公開鍵暗号システムを利用して署名の生成および検証を行うＲＳＡ署名生成・検証部７１や、ＤＳＡ（Digital Signature Algorithm）方式を利用して署名の生成および検証を行うＤＳＡ署名生成・検証部７２が備えられている。

【００６０】ＲＳＡ署名生成・検証部７１では、２つの鍵によって暗号化と復号を行う。ＲＳＡ暗号系では、２つの鍵は、例えば、次のようにして決められる。

【００６１】ある２つの大きな素数pとqを選んで、その積n＝pqを求める。そして、（p－1）×（q－1）以下で（p－1）×（q－1）と互いに素な整数eを選び、次の式（１）を満たす整数dを求める。

$e \times d = 1 \bmod ((p-1) \times (q-1)) \cdots (1)$

すると（e，n）が公開鍵、dが秘密鍵となる。

【００６２】文Mを暗号化して、暗号化データCを生成する場合、次の式（２）を用いる。

$C = M^e \bmod n \cdots (2)$

また、暗号化データCを復号する場合、次の式（３）を用いる。

$M = C^d \bmod n \cdots (3)$

【００６３】ＤＳＡ署名生成・検証部７２には、図示しない乱数生成部が備えられている。ＤＳＡは、DLP（Discrete Logarithm Problem:離散対数問題）の困難性をベースとしたElGamal署名を改良して、署名の長さを160bit×2に短縮し、署名鍵の生成等を特定の方法で運用するデジタル署名アルゴリズムである。署名生成において、ハッシュ関数（データ圧縮関数）にSHA－１（Secure Hash Algorithm－1）を使うことを前提としている。ＤＳＡ方式は、米国政府機関であるNIST（米国商務省標準技術局：National Institute of Standards and Technology）により、電子署名の標準として開発され、米国連邦情報処理標準（Federal Information Processing Standard）FIPS PUB 186に定められた。

【００６４】また、図５（Ｂ）に示されるように、共通鍵処理部４２には、例えば、ＤＥＳ（Data Encryption Standard）共通鍵暗号システムによる認証処理を行うＤＥＳ処理部７３、ＲＣ５（Rivest Cipher５）方式による認証処理を行うＲＣ５処理部７４、およびＡＥＳ（Advanced Encryption Standard）方式による認証処理を行

うＡＥＳ処理部７５が備えられている。

【００６５】ＤＥＳ共通鍵暗号システムは、1977年にNISTで制定され、1981年に米国規格協会（ANSI：American National Standards Institute）により標準化された共通鍵暗号システムである。ＤＥＳ共通鍵暗号システムの鍵の認証アルゴリズムは公開されており、共通鍵暗号システムの代表として広く普及している。

【００６６】ＤＥＳ共通鍵暗号システムは、データを64bit単位に区切って暗号化および復号処理を行う暗号システムである。ＤＥＳアルゴリズムにおいては、暗号化と復号は対称をなしており、受信した暗号文を同じ鍵を使ってもう一度変換すれば元の文章が復元できる。また、ＤＥＳ共通鍵暗号システムでは、簡単なビット位置転置とXOR演算の組み合わせ論理を16回繰り返している。内部的にはデータのフィードバックや条件判断部分がなく、処理が逐次的なので、パイプライン化すれば高速に処理することができる。もともとLSI化することを前提にして決められたアルゴリズムであり、ＤＥＳチップも多く作られている。

【００６７】ＲＣ５とは、ＲＳＡ Data Security社と、マサチューセッツ工科大学が開発したRCシリーズの共通鍵暗号方式であり、1995年に提案された。ＲＣ５は、可変長ブロックサイズ、可変長の鍵サイズ、および可変長回数（元データや鍵によって、ビット回転の量が変わる、Data-dependent-rotations（データ依存ビット回転）アルゴリズム）のラウンドを有するブロック暗号化方式である。そのブロックサイズとしては、32、64、128ビットをとることが可能であり、ラウンド数は0から255、鍵サイズは0から2048ビットまで可変である。ＲＣ５のアルゴリズムは公開されていて、RFC2040 として入手することが可能である。

【００６８】また、ＡＥＳ方式は、NISTによって選定作業が行われている、米国政府の次世代標準暗号化方式である。現在標準暗号として用いられているＤＥＳが制定されたのは1977年であり、近年のコンピュータの高性能化、暗号理論の発展に伴い、その信頼性は年々低下している。そこで、NISTはＤＥＳに代わる次世代の暗号標準として、ＡＥＳ候補となる暗号方式を全世界から公募した。世界中から集まった１５の方式が審査を受けており、２１世紀初頭までに決定される予定である。

【００６９】そして、その他の暗号処理部４３は、例えば、デジタル署名を用いる場合に、メッセージに対して、不可逆的なハッシュ関数を作用させることで、「メッセージダイジェスト」を作成し、メッセージダイジェストを署名鍵により暗号化することによって、デジタル署名を作成する等の、公開鍵処理部４１もしくは共通鍵処理部４２が処理する以外の暗号処理を実行する。その他の暗号処理部４３には、図５（Ｃ）に示されるように、例えば、署名生成および署名検証に用いられるハッシュ関数SHA-1の処理を行うSHA-1処理部７６、および相互認証プロトコルで利用される真性乱数を生成する真性乱数生成部７７が備えられるか、あるいは、図５（Ｄ）に示されるように、署名生成および署名検証に用いられるハッシュ関数ＭＤ５の処理を行うＭＤ５処理部７８、および相互認証プロトコルで利用される擬似乱数（ある有限な桁数の数字の範囲で出来るだけランダムな数字列をもつ人工的な乱数）を生成する擬似乱数生成部７９が備えられている。

【００７０】デジタル署名においては、公開鍵暗号方式を用いるため、処理速度が遅いことが問題となるが、メッセージダイジェストを作成することによって、デジタル署名作成にかかる時間が削減される。更に、ハッシュ関数は、データの改ざんに対して大きく反応する特性を有していることから、デジタル署名を検証する際に、デジタル署名を検証鍵で復号して取り出したメッセージダイジェストと、送られてきたメッセージ本文にハッシュ関数を作用させて作成したメッセージダイジェストを比較することにより、メッセージ本文が改ざんされていないかどうかを容易に確認することができる。

【００７１】SHA-1は任意の長さのメッセージから160bitのハッシュ値を生成する一方向ハッシュ関数である。ＤＳＡ同様、NISTが開発したもので、NISTによってFIPS PUB180 に定められた。標準原案（N544）は、基本的にFIPS PUB 180に準拠したものとなっている。

【００７２】そして、ＭＤ５は、広く一般に使われているメッセージダイジェスト関数アルゴリズムのうちの１つで、RFC1321で定義されている。ＭＤ５は、32bitコンピュータ上で効率よく計算できるように、アルゴリズムが決められている。ほかにＭＤ４やＭＤ２という、類似のアルゴリズムもある。

【００７３】次に、図６を用いて、図３および図４を用いて説明したＩＣカード１のＳＲＡ４６に格納されている情報について説明する。

【００７４】ＳＲＡ４６は、ＩＣカード１を保有するユーザが、図２を用いて説明した一般リーダライタ２－１２などを用いて、複数のサービスを受けることができるようにするために、それらの複数のサービスを受けるための情報（図２を用いて説明したサービス登録用リーダライタ２－１１を用いて登録された情報）を記録するためのメモリ領域である。

【００７５】すなわち、ＳＲＡ４６には、そのＩＣカード１に登録されているサービスの情報であるService Individual Info1 乃至Nが登録されており、それぞれのService Individual Infoには、サービスの種類を識別するためのサービスＩＤ、サービス毎に予め定められた、１つ、もしくは複数の認証用鍵情報（図６におけるService Individual Info kにおいては、１乃至nのn個の認証用鍵情報）、サービスを受けるために利用されるサービスデータ、および、鍵情報をバージョンアップするための認証鍵Kake_vupと、必要に応じて、認証鍵に対す

る証明書などが登録されている。

【００７６】認証用鍵情報には、例えば、認証鍵ＩＤ、鍵のレベルおよびバージョン、認証方式、および、複数の認証鍵を識別するために用いられる識別用認証鍵Kake（必要に応じて、認証鍵に対する証明書）などが含まれる。また、サービスデータには、ユーザＩＤ以外に、Service Individual Info kが、例えば、電子マネーサービスである場合、電子マネーの残高情報や累積ポイント等、Service Individual Info kが、例えば、自動改札サービスである場合、有効区間情報等が格納される。

【００７７】次に、図７を用いて、図６のService Individual Infoに登録される認証用鍵情報について説明する。

【００７８】図７（Ａ）においては、領域No．１および領域No．２のそれぞれに対応して、認証鍵ＩＤ、鍵のバージョン、認証方式、識別用認証鍵Kake、および、必要に応じて、証明書データが登録されている。図７（Ａ）のように認証用鍵情報が登録されている場合の認証鍵識別処理については、図２０乃至図２４を用いて後述する。

【００７９】図７（Ｂ）においては、領域No．１乃至領域No．７のそれぞれに対応して、認証鍵ＩＤ、鍵のレベル、鍵のバージョン、認証方式、識別用認証鍵Kake、および、必要に応じて、証明書データが登録されている。図７（Ｂ）のように、鍵のレベルを含んだ認証用鍵情報が登録されている場合の認証鍵識別処理については、図２７および図２８を用いて後述する。

【００８０】次に、図８を用いて、図３および図４を用いて説明したＩＣカード１のＳＲＴ４５に格納されている情報について説明する。

【００８１】ＳＲＴ４５には、ＩＤカード１に複数のサービスが登録されている場合に、あるサービスを行いながら別のサービスのサービスデータに対してアクセスを許可するためのデータが登録されている。ＳＲＴ４５は、ＩＣカード１に登録されているサービスＩＤが記載されている登録サービスＩＤフィールド（図８においては、サービスＩＤＡ乃至Ｊとして記載されている）と、それぞれのサービスＩＤに対応するパーミッション情報が記載されているパーミッション情報フィールドで構成されている。

【００８２】パーミッション情報の登録サービスＩＤフィールドには、登録されているサービスのサービスＩＤがすべて列挙されている。そして、パーミッション情報フィールドには、対応するサービスが実行されている場合に、登録サービスＩＤフィールドに記載されているサービスにアクセスすることができるサービスＩＤと、どのような処理を行うことを許可するかを示す情報が記載されている。例えば、読み出しおよび書き込みが許可されている場合、パーミッション情報として「ｒｗ」が記載され、読み出しのみ許可されている場合、パーミッション情報として「ｒｏ」が記載され、鍵のバージョンアップが許可されている場合、パーミッション情報として「ｖｕｐ」が記載される。「ｒｗ」と「ｒｏ」は同じサービスＩＤに対して許可されないが、「ｒｗ」と「ｖｕｐ」および「ｒｏ」と「ｖｕｐ」は、同じサービスＩＤに対して許可され、パーミッション情報フィールドに列挙することが可能である。

【００８３】すなわち、ＳＲＴ４５に、図８に示されるパーミッション情報が登録されている場合、サービスＩＤがＣで示されるサービスの実行中には、サービスＩＤがＢで示されるサービスに対して、読み出し、および書き込みが許可され、更に、サービスＩＤがＤで示されるサービスの実行中においても、サービスＩＤがＢで示されるサービスに対しての読み出しが許可され、サービスＩＤがＥで示されるサービスの実行中に、サービスＩＤがＤで示されるサービスに対して、読み出し、書き込み、および鍵のバージョンアップが許可され、以下、サービスＩＤがＥで示されるサービス、サービスＩＤがＦで示されるサービス、サービスＩＤがＧで示されるサービス、もしくは、サービスＩＤがＩで示されるサービスにおいても、対応するパーミッション情報フィールドに記載されている情報に基づいて、他のサービスＩＤに対応する処理の実行中に、パーミッション情報に対応した処理が許可される。

【００８４】これらのパーミッション情報の登録は、ＩＣカード１に、対応するサービスを登録する場合に行われる。すなわち、ユーザが、サービス登録用リーダライタ２－１１を用いて、自分自身が保有するＩＣカード１に対して、サービスＩＤがＦで示されるサービスを登録する場合、例えば、サービスＩＤがＧで示されるサービスがすでに登録され、サービスＩＤがＨで示されるサービスが登録されていないならば、登録サービスＩＤフィールドのＦに対応するパーミッション情報フィールドには、サービスＩＤがＧで示されるサービスに対応するパーミッション情報しか登録することができない。そして、ユーザが、サービスＩＤがＨで示されるサービスをＩＤカード１に登録した後、サービスＩＤがＦで示されるサービスをアップデートすることにより、サービスＩＤがＦで示されるサービスに対する、サービスＩＤがＨで示されるサービスのパーミッション情報を登録することができる。

【００８５】次に、図９は、リーダライタ２の構成を示すブロック図である。

【００８６】リーダライタ２は、ＩＣカード１との通信を行う通信部９１と、データ処理を実行するリーダライタ処理部９２から構成されている。

【００８７】通信部９１は、ＩＣカード１との通信方法によって（すなわち、リーダライタ２が、図１を用いて説明した非接触式と接触式のいずれの通信方式を採用しているかによって）、電磁波を用いて通信するためのコ

イルのみを備えるか、もしくは、電磁波を用いて通信するためのコイル、および接触式により通信するための接触端子を備える構造を有している。

【００８８】通信部９１は、ＩＣカード１から送信されたデータを受信し、受信したデータが、例えば、ＡＳＫやＢＰＳＫを用いて変調されている場合、所定の処理により、受信したデータを復調し、リーダライタ処理部９２の制御部１０１に供給するとともに、リーダライタ処理部９２の処理により生成されたデータを、制御部１０１から供給され、ＡＳＫやＢＰＳＫを用いて変調し、ＩＣカード１に送信する。

【００８９】リーダライタ処理部９２は、制御部１０１、暗号処理部１０２、メモリ１０３、通信部１０４、表示部１０５、および入力部１０６より構成されている。制御部１０１は、通信部９１から供給されたデータに従って、暗号処理部１０２を制御し、ＩＣカード１との認証処理等に必要な暗号処理を実行させたり、必要に応じて、メモリ１０３に記録されているデータを読み込んで、通信部９１を介して、ＩＣカード１に送信したり、ユーザが入力部１０６を用いて入力した各種操作に対応した信号や、ネットワークを介して、通信部１０４に入力された制御信号の入力を受け、これらの信号に従って、処理を実行し、その結果を表示部１０５に表示させる。

【００９０】また、通信部１０４には、ドライブ１１４も接続されており、ドライブ１１４に装着される磁気ディスク１１５、光ディスク１１６、光磁気ディスク１１７、および半導体メモリ１１８などとデータの授受を行ことができる。

【００９１】暗号処理部１０２は、図３を用いて説明した暗号処理部３３と同様の構成を有しているので、その説明は省略する。

【００９２】メモリ１０３には、ＩＣカード１と所定の処理を実行するための情報が記憶されている。その情報は、リーダライタ２が、図２を用いて説明した、サービス登録用リーダライタ２－１１乃至バージョンアップ用リーダライタ２－１４のいずれに対応するものであるかによって異なる。図１０乃至図１４を用いて、サービス登録用リーダライタ２－１１乃至バージョンアップ用リーダライタ２－１４のメモリ１０３に記憶されているデータについて説明する。

【００９３】図１０に示される、サービス登録用リーダライタ２－１１のメモリ１０３には、ＩＣカード１のメモリ３２のＳＲＡ４６にデータを登録もしくは削除する場合に用いられる認証鍵Kregが記憶され（必要に応じて認証鍵の証明書も記憶されている）、ＩＣカード１に登録するための各種サービスに対応するService Individual Info1乃至nが記憶されている。

【００９４】図１１に示される、一般リーダライタ２－１２のメモリ１０３には、この一般リーダライタ２－１２で処理することが可能なサービスに対応するサービスＩＤと、それに対応する認証鍵リスト、および鍵失効情報が記憶されている。また、一般リーダライタ２－１２に、鍵バージョンアップのサービスを可能とさせる場合、一般リーダライタ２－１２のメモリ１０３には、新バージョンの鍵などの情報も、あわせて記憶される。

【００９５】図１２に示される、モジュール間通信用リーダライタ２－１３のメモリ１０３には、一般リーダライタ２－１２のメモリ１０３に記憶されている情報と同様に、このモジュール間通信用リーダライタ２－１３で処理することが可能なサービスに対応するサービスＩＤと、それに対応する認証鍵リスト、および鍵失効情報が記憶されている。モジュール間通信とは、図１３に示されるように、共通鍵方式および公開鍵方式の２方式に対応するようになされているモジュール間通信用リーダライタ２－１３に、公開鍵モジュール１２１（例えば、図４を用いて説明した、ＩＣカード１の通信部５３および公開鍵サービス処理部５４に対応する）と、共通鍵モジュール１２２（例えば、図４を用いて説明したＩＣカード１の通信部５１および共通鍵サービス処理部５２に対応する）を有するＩＣカード１を装着し、公開鍵モジュール１２１と共通鍵モジュール１２２とのデータの通信を、モジュール間通信用リーダライタ２－１３を介して行うことである。モジュール間通信に関する処理の詳細は、図４８乃至図５１を用いて後述する。

【００９６】そして、図１４に示される、バージョンアップ用リーダライタ２－１４のメモリ１０３には、装着されたＩＣカード１に登録されているサービスの認証鍵をバージョンアップするための、サービスＩＤと、そのサービスＩＤに対応するバージョンアップ用認証鍵Kake_vupおよび認証鍵Kakeのリストが記憶されている。

【００９７】ＩＣカード１とリーダライタ２とが通信を行う場合、いくつかの例外となる処理を除いて、はじめに、ＩＣカード１とリーダライタ２が相互認証するために、通信を行うサービスを相互に識別し、そのサービスの認証鍵を相互に識別する必要がある。図１５のフローチャートを参照して、ＩＣカード１とリーダライタ２の相互認証処理について説明する。

【００９８】まず、ステップＳ１において、リーダライタ２は、必要に応じて、ＩＣカード１と通信して必要なデータの授受を行うことにより、図１６および図１８を用いて後述するリーダライタ２のサービス識別処理を実行する。そして、ステップＳ２において、ＩＣカード１は、必要に応じて、リーダライタ２と通信して必要なデータの授受を行うことにより、図１７および図１９を用いて後述するＩＣカード１のサービス識別処理を実行する。

【００９９】そして、ステップＳ１のリーダライタ２のサービス識別処理およびステップＳ２のＩＣカード１のサービス識別処理が正常終了した場合、ステップＳ３に

おいて、リーダライタ２は、必要に応じて、ＩＣカード１と通信して必要なデータの授受を行うことにより、図２０、図２２および図２７を用いて後述するリーダライタ２の認証鍵識別処理を実行する。そして、ステップＳ４において、ＩＣカード１は、必要に応じて、リーダライタ２と通信して必要なデータの授受を行うことにより、図２１、図２３および図２８を用いて後述するＩＣカード１の認証鍵識別処理を実行する。

【０１００】次に、図１６のフローチャートを参照して、複数のサービスに対応しているＩＣカード１と、複数のサービスに対応しているリーダライタ２において、ユーザが所望のサービスを入力し、そのサービスの実行が可能か否かを判断することにより、図１５のステップＳ１において実行されるリーダライタ２のサービス識別処理について説明する。

【０１０１】リーダライタ２の制御部１０１は、ステップＳ１１において、ＩＣカード１に対し、通信部９１を介して、ＩＣカード検出コマンドを送信し、ステップＳ１２において、ＩＣカード１からＡＣＫ信号（後述する図１７のステップＳ２２において、ＩＣカード１が送信した信号）を受信したか否かを判断する。ステップＳ１２において、ＡＣＫ信号が受信されていないと判断された場合、ＡＣＫ信号が受信されたと判断されるまで、ステップＳ１２の処理が繰り返される。

【０１０２】ステップＳ１２において、ＡＣＫ信号を受信したと判断された場合（すなわち、ＩＣカード１が、リーダライタ２に装着された場合）、ステップＳ１３において、制御部１０１は、ユーザが入力部１０６を用いて入力した操作を示す信号に従って、または、予め決められたサービスに基づいて、ユーザが希望するサービスに対応するサービスＩＤを、通信部９１を介して、ＩＣカード１に送信する。

【０１０３】ステップＳ１４において、制御部１０１は、ＩＣカード１から送信される信号（後述する図１７のステップＳ２５もしくはステップＳ２６において、ＩＣカード１が送信した信号）を受信する。ステップＳ１５において、制御部１０１は、ステップＳ１４において受信したデータは、ＡＣＫ信号か否かを判断する。ステップＳ１５において、受信した信号がＡＣＫ信号ではない（すなわちＮＡＣＫ信号である）と判断された場合、ステップＳ１６において、制御部１０１は、エラーメッセージに対応するデータを表示部１０５に出力して表示させ、処理を終了する（すなわち、処理は、図１５のステップＳ３には進まない）。ステップＳ１５において、受信した信号がＡＣＫ信号であると判断された場合、処理は、図１５のステップＳ３に進む。

【０１０４】次に、図１７のフローチャートを参照して、図１５のステップＳ２において、図１６を用いて説明したリーダライタ２のサービス識別処理と並行して実行される、ＩＣカード１のサービス識別処理について説明する。なお、ここでは、図３を用いて説明したＩＣカード１において処理が行われるものとして説明するが、図４を用いて説明したＩＣカード１によって処理が実行される場合においても、基本的に同様の処理が実行される。

【０１０５】ＩＣカード１の制御部３１は、ステップＳ２１において、図１６のステップＳ１１において、リーダライタ２が送信したＩＣカード検出コマンドを、通信部２１を介して受信し、ステップＳ２２において、リーダライタ２にＡＣＫ信号を送信する。

【０１０６】制御部３１は、ステップＳ２３において、図１６のステップＳ１３において、リーダライタ２が送信したサービスＩＤを、通信部２１を介して受信し、ステップＳ２４において、受信したサービスＩＤは、ＩＣカード１の対応するモジュール（ここでは、図３を用いて説明したＩＣカード１における処理について説明しているので、ＩＣカード処理部２２のメモリ３２に対応するが、例えば、図４を用いて説明したＩＣカード１の場合、リーダライタ２が対応している方式により、共通鍵サービス処理部５２のメモリ６２あるいは、公開鍵サービス処理部のメモリ６２に対応する）内に登録されているＩＤであるか否か、すなわち、ステップＳ２３において受信したサービスＩＤが、図６を用いて説明したＳＲＡ４６に登録されているか否かを判断する。

【０１０７】ステップＳ２４において、受信したサービスＩＤが、モジュール内に登録されていると判断された場合、ステップＳ２５において、制御部３１は、通信部２１を介して、リーダライタ２にＡＣＫ信号を送信し、処理は、図１５のステップＳ４に進む。ステップＳ２４において、受信したサービスＩＤが、モジュール内に登録されていないと判断された場合、ステップＳ２６において、制御部３１は、通信部２１を介して、リーダライタ２にＮＡＣＫ信号を送信し、処理が終了される（すなわち、図１５のステップＳ４には進まない）。

【０１０８】次に、図１８のフローチャートを参照して、複数のサービスに対応しているＩＣカード１と、複数のサービスに対応しているリーダライタ２において、該当するＩＣカード１とリーダライタ２が実行可能なサービスを抽出して、リーダライタ２の表示部１０５に表示させ、それらのサービスの中から、ユーザが所望するサービスを選択させることにより、サービス識別を行う場合における、図１５のステップＳ１において実行される、リーダライタ２のサービス識別処理について説明する。

【０１０９】リーダライタ２の制御部１０１は、ステップＳ３１において、サービスＩＤリスト送信コマンドを、ＩＣカード１に、通信部９１を介して送信し、ステップＳ３２において、後述する図１９のステップＳ５２において、ＩＣカード１が送信した、サービスＩＤリストを受信したか否かを判断する、ステップＳ３２におい

て、サービスＩＤリストを受信していないと判断された場合、サービスＩＤリストを受信したと判断されるまで、ステップＳ３２の処理が繰り返される。

【０１１０】ステップＳ３２において、サービスＩＤリストを受信したと判断された場合、ステップＳ３３において、制御部１０１は、受信したサービスＩＤリストに記載されているサービスＩＤは、リーダライタ２が対応しているサービスが含まれているか否か（すなわち、リーダライタ２のメモリ１０３に記憶されているサービスＩＤを含んでいるか否か）を判断する。

【０１１１】ステップＳ３３において、受信したサービスＩＤリストに、リーダライタ対応サービスが含まれていると判断された場合、ステップＳ３４において、制御部１０１は、サービスＩＤリストに含まれていた対応サービスが複数であるか否かを判断する。ステップＳ３４において、対応サービスが複数ではない（すなわち１つだけである）と判断された場合、処理は、ステップＳ３７に進む。

【０１１２】ステップＳ３４において、対応サービスが複数であると判断された場合、制御部１０１は、ステップＳ３５において、複数の対応サービスを表示部１０５に表示させるためのデータを生成し、表示部１０５に出力して表示させ、ステップＳ３６において、入力部１０６から、ユーザが希望するサービスの入力を受ける。あるいは、サービスそれぞれに、優先度情報を含ませておき、複数の対応サービスのうちから、優先度の最も高いサービスが自動的に選択されるようにしてもよい。

【０１１３】ステップＳ３７において、制御部１０１は、ステップＳ３４において、対応サービスがただ１つであると判断された場合は、そのサービスに対応するサービスＩＤを、ステップＳ３４において、対応サービスが複数であると判断された場合は、ステップＳ３６において、ユーザが入力部１０６を用いて入力した希望するサービスに対応するサービスＩＤを、通信部９１を介して、ＩＣカード１に送信し、処理は、図１５のステップＳ３に進む。

【０１１４】ステップＳ３３において、受信したサービスＩＤリストに、リーダライタ対応サービスが含まれていないと判断された場合、制御部１０１は、ステップＳ３８において、通信部９１を介して、ＩＣカード１にＮＡＣＫ信号を送信し、ステップＳ３９において、図１６のステップＳ１６と同様の処理がなされ、処理が終了される（すなわち、処理は、図１５のステップＳ３には進まない）。

【０１１５】次に、図１９のフローチャートを参照して、図１５のステップＳ２において、図１８を用いて説明したリーダライタ２のサービス識別処理と並行して実行される、ＩＣカード１のサービス識別処理について説明する。なお、ここでは、図３を用いて説明したＩＣカード１において処理が行われるものとして説明するが、図４を用いて説明したＩＣカード１によって処理が実行される場合においても、基本的に同様の処理が実行される。

【０１１６】ＩＣカード１の制御部３１は、ステップＳ５１において、リーダライタ２が、図１８のステップＳ３１において送信したサービスＩＤ送信コマンドを、通信部２１を介して受信し、ステップＳ５２において、自分自身が対応しているサービスＩＤリスト（すなわち、メモリ３２のＳＲＡ４６に登録されているサービスＩＤのリスト）を生成して、通信部２１を介して、リーダライタ２に送信する。

【０１１７】制御部３１は、ステップＳ５３において、リーダライタ２が、図１８のステップＳ３７もしくはステップＳ３８において、ＩＣカード１に送信したデータを、通信部２１を介して受信し、ステップＳ５４において、リーダライタ２から受信したデータはＮＡＣＫ信号か否かを判断する。ステップＳ５４において、受信した信号がＮＡＣＫ信号であると判断された場合（すなわち、受信したデータが、図１８のステップＳ３８において、リーダライタ２がＩＣカード１に送信した信号である場合）、処理が終了される（すなわち、処理は、図１５のステップＳ４には進まない）。

【０１１８】ステップＳ５４において、リーダライタ２から受信したデータはＮＡＣＫ信号ではないと判断された場合（すなわち、受信したデータが、図１８のステップＳ３７において、リーダライタ２がＩＣカード１に送信したサービスＩＤである場合）、ステップＳ５５において、制御部３１は、リーダライタ２から受信したサービスＩＤは、自分自身のメモリ３２のＳＲＡ４６に登録されているか否か判断する。

【０１１９】ステップＳ５５において、サービスＩＤが登録されていないと判断された場合、処理が終了される（すなわち、処理は、図１５のステップＳ４には進まない），ステップＳ５５において、サービスＩＤが登録されていると判断された場合、処理は、図１５のステップＳ４に進む。

【０１２０】次に、図２０のフローチャートを参照して、図７（Ａ）を用いて説明した認証用鍵情報を用いて認証鍵識別が行われる場合、図１５のステップＳ３において実行される、リーダライタ２の認証鍵識別処理について説明する。

【０１２１】リーダライタ２の制御部１０１は、ステップＳ６１において、図１５のステップＳ１およびステップＳ２のサービス識別処理により識別されたサービスに対応するサービスＩＤ（ここでは、対応するサービスＩＤを、ＩＤ_Ｓとする）に属する認証鍵のうちの１つに対応する認証鍵ＩＤを、メモリ１０３から読み出し、通信部９１を介して、ＩＣカード１に送信し、ステップＳ６２において、後述する図２１のステップＳ７３もしくはステップＳ７５において、ＩＣカード１が送信するデ

ータを受信する。

【0122】ステップS63において、制御部101は、ステップS62において、ICカード1から受信したデータは、ACK信号か否かを判断する。ステップS63において、ACK信号が受信されたと判断された場合、ステップS64において、制御部101は、暗号処理部33を制御して、ステップS61において、暗号処理部102の公開鍵処理部111もしくは共通鍵処理部112のうち、ICカード1に送信した認証鍵IDに対応する認証鍵を用いて認証処理を行う処理部を選択して制御することにより、ICカード1との相互認証処理および鍵共有処理を開始し、ICカード1とセッション鍵Ksesを共有し、相互認証処理が終了した後、処理が終了される。

【0123】ステップS63において、ACK信号が受信されていないと判断された場合（すなわち、NACK信号を受信したと判断された場合）、ステップS65において、図16のステップS16と同様の処理がなされ、処理が終了される。

【0124】次に、図21のフローチャートを参照して、図15のステップS4において、図20のリーダライタ2の認証鍵識別処理と並行して実行される、ICカード1の認証鍵識別処理について説明する。なお、ここでも、図3を用いて説明したICカード1により、処理が実行される場合について説明するが、図4を用いて説明したICカード1によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0125】ICカード1の制御部31は、ステップS71において、図20のステップS61において、リーダライタ2が送信した認証鍵IDを、通信部21を介して受信し、ステップS72において、ステップS71において受信した認証鍵IDは、メモリ32のSRA46のID_Sに関するデータが記憶されている領域に登録されているか否かを判断する。

【0126】ステップS72において、認証鍵IDが登録されていると判断された場合、制御部31は、ステップS73において、通信部21を介して、リーダライタ2にACK信号を送信し、ステップS74において、暗号処理部33の公開鍵処理部41もしくは共通鍵処理部42のうち、リーダライタ2に指定された認証鍵による認証処理を行う方を選択して制御することにより、相互認証処理を実行し、リーダライタ2とセッション鍵Ksesを共有し、相互認証処理の終了後、処理が終了される。ステップS72において、認証鍵IDが登録されていないと判断された場合、ステップS75において、制御部31は、通信部21を介して、リーダライタ2にNACK信号を送信し、処理が終了される。

【0127】図20および図21を用いて説明した処理においては、ICカード1とリーダライタ2は、図15のステップS1およびステップS2の処理により識別されたサービスのサービスIDに対応する、リーダライタ2が指定した認証鍵により、相互認証を実行する。

【0128】例えば、あるサービスに対して共通鍵および公開鍵の2種類の認証鍵が用意されている場合、共通鍵に基づく認証処理により高速な処理を行うことをデフォルトとし、共通鍵のバージョンが古い場合には、公開鍵に基づいて認証処理を実施するようにしてもよい。

【0129】次に、図22のフローチャートを参照して、図15のステップS3において実行される、図15のステップS1およびステップS2の処理により識別されたサービスのサービスIDに対応するサービスに対して、共通鍵および公開鍵の2種類の認証鍵が用意されている場合のリーダライタ2の認証鍵識別処理について説明する。

【0130】リーダライタ2の制御部101は、ステップSS1において、図15のステップS1およびステップS2の処理により識別されたサービスのサービスIDに対応する認証鍵の、共通鍵バージョン情報要求コマンドを、通信部91を介してICカード1に送信し、ステップSS2において、後述する図23のステップS92において、ICカード1が送信した共通鍵バージョン情報を、通信部91を介して受信する。

【0131】ステップSS3において、制御部101は、ステップSS2において受信した共通鍵バージョン情報を基に、共通鍵バージョンが有効か否かを判断する。ステップSS3において、共通鍵バージョンが有効であると判断された場合、ステップSS4において、制御部101は、ICカード1に、共通鍵による相互認証開始コマンドを送信し、暗号処理部102の共通鍵処理部112を制御して、共通鍵による相互認証を開始し、ICカード1とセッション鍵Ksesを共有し、相互認証が終了した後、処理が終了される。

【0132】ステップSS3において、共通鍵バージョンが有効ではないと判断された場合、ステップSS5において、制御部101は、ICカード1に、公開鍵による相互認証開始コマンドを送信し、暗号処理部102の公開鍵処理部111を制御して、公開鍵による相互認証を開始し、ICカード1とセッション鍵Ksesを共有し、相互認証が終了した後、処理が終了される。

【0133】次に、図23のフローチャートを参照して、図15のステップS4において、図22を用いて説明したリーダライタ2の認証鍵識別処理と並行して実行される、ICカード1の認証鍵識別処理について説明する。なお、ここでも、図3を用いて説明したICカード1により、処理が実行される場合について説明するが、図4を用いて説明したICカード1によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0134】ICカード1の制御部31は、ステップS91において、図22のステップSS1において、リー

ダライタ2が送信した共通鍵バージョン情報要求コマンドを受信し、ステップS92において、共通鍵バージョン情報を、通信部21を介して、リーダライタ2に送信する。

【0135】制御部31は、ステップS93において、図22のステップS84もしくはステップS85において、リーダライタ2が送信した相互認証開始コマンドを受信し、ステップS94において、ステップS93において受信された相互認証開始コマンドは、共通鍵による相互認証開始コマンドであるか否かを判断する。

【0136】ステップS94において、共通鍵による相互認証開始コマンドであると判断された場合、ステップS95において、制御部31は、暗号処理部33の共通鍵処理部42を制御して、共通鍵による相互認証を開始し、リーダライタ2とセッション鍵Ksesを共有し、相互認証が終了した後、処理が終了される。

【0137】ステップS94において、共通鍵による相互認証開始コマンドではない（すなわち、公開鍵による相互認証開始コマンドである）と判断された場合、ステップS96において、制御部31は、暗号処理部33の公開鍵処理部41を制御して、公開鍵による相互認証を開始し、リーダライタ2とセッション鍵Ksesを共有し、相互認証が終了した後、処理が終了される。

【0138】図22および図23を用いて説明した処理により、ICカード1とリーダライタ2は、まず、認証速度の速い共通鍵による相互認証を実行しようとし、共通鍵による相互認証が行えない場合（例えば、対応する共通鍵のバージョンが古い場合や、第3者に認証鍵が漏洩してしまった場合など）、公開鍵を用いて、相互認証を実行する。

【0139】図22のステップS85および図23のステップS96の処理においては、公開鍵による相互認証が行われる。リーダライタ2のメモリ103のSRA46には、図24（A）に示されるリーダライタ2の証明書が記憶されている。また、ICカード1のメモリ32のSRA46には、図24（B）に示されるICカード1の証明書が記憶されている。

【0140】図24（A）および図24（B）に示されるように、それぞれの証明書には、証明書のバージョン番号、認証局が割り付ける証明書の通し番号、署名に用いたアルゴリズムとパラメータ、認証局の名前、証明書の有効期限、リーダライタ2、あるいはICカード1の名前（ID）、リーダライタ2の公開鍵Kpsp、あるいはICカード1の公開鍵Kpu、およびメッセージ全体に、図5を用いて説明したような不可逆的なハッシュ関数（データ圧縮関数）を作用させることで、メッセージダイジェストを作成し、メッセージダイジェストを、認証局の秘密鍵Kscaにより暗号化することによって作成された、デジタル署名から構成される。

【0141】次に、図25のフローチャートを参照して、署名生成処理について説明する。ここでは、楕円曲線暗号方式（楕円DSA署名）を用いて、デジタル署名を生成する場合について説明する。ここでは、ICカード1の制御部31が、公開鍵処理部41のDSA署名生成・検証部72を制御することにより実行される処理について説明するが、リーダライタ2においても、同様の処理が実行されるので、リーダライタ2の処理についての説明は省略する。

【0142】ステップS101において、制御部31は、署名生成処理に必要なパラメータを認識する。すなわち、pを標数、aおよびbを楕円曲線の係数、楕円曲線を$y^2=x^3+ax+b$、Gを楕円曲線上のベースポイント、rをGの位数、Mをメッセージ、Ksを秘密鍵、GおよびKsGを公開鍵とする。

【0143】公開鍵処理部41のDSA署名生成・検証部72は、ステップS102において、図示しない乱数生成部で、$0<u<r$となるuを生成し、ステップS103において、ステップS102において生成された乱数uを用いて、公開鍵Gをu倍し、$V=uG=(Xv, Yv)$となるVを算出する。

【0144】DSA署名生成・検証部72は、ステップS104において、$c=Xv \bmod r$を算出し、ステップS105において、S104の計算結果に基づいて、c=0であるか否かを判断する。ステップS105において、c=0であると判断された場合、処理は、ステップS102に戻り、それ以降の処理が繰り返される。

【0145】ステップS105において、c=0ではないと判断された場合、DSA署名生成・検証部72は、ステップS106において、メッセージMのハッシュ値であるf=SHA-1（M）（ここでは、ハッシュ関数として、SHA-1が用いられる）を算出し、ステップS107において、$d=[(f+cKs)\cdot u] \bmod r$を計算する。

【0146】ステップS108において、DSA署名生成・検証部72は、ステップS107の計算結果に基づいて、d=0か否かを判断する。ステップS108において、d=0であると判断された場合、処理は、ステップS102に戻り、それ以降の処理が繰り返される。ステップS108において、d=0ではないと判断された場合、ステップS109において、DSA署名生成・検証部72は、署名データを（c，d）とし、処理が終了される。

【0147】このようにしてICカード1において生成されたデジタル署名を受信したリーダライタ2は、受信したデジタル署名を検証する処理を実施する。図26のフローチャートを参照して、署名検証処理について説明する。ここでは、リーダライタ2の制御部101が、公開鍵処理部41のDSA署名生成・検証部72を制御することにより実行される処理について説明するが、ICカード1においても、同様の処理が実行されるので、I

Cカード1の処理についての説明は省略する。

【0148】ステップS111において、制御部101は、署名生成処理に必要なパラメータを認識する。すなわち、pを標数、aおよびbを楕円曲線の係数、楕円曲線を$y^2=x^3+ax+b$、Gを楕円曲線上のベースポイント、rをGの位数、Mをメッセージ、Ksを秘密鍵、GおよびKsGを公開鍵とする。

【0149】公開鍵処理部41のDSA署名生成・検証部72は、ステップS112において、受信した署名データのcおよびdの値に基づいて、$0<c<r$かつ$0<d<r$であるか否かを判断する。

【0150】ステップS112において、$0<c<r$かつ$0<d<r$ではないと判断された場合、処理はステップS120に進む。ステップS112において、$0<c<r$かつ$0<d<r$であると判断された場合、ステップS113において、DSA署名生成・検証部72は、メッセージMのハッシュ値であるf=SHA-1(M)を算出し、ステップS114において、$h=1/d \bmod r$を計算する。

【0151】DSA署名生成・検証部72は、ステップS114において算出されたhの値を用いて、ステップS115において、$h1=fh$、$h2=ch \bmod r$を算出し、ステップS116において、$P=(Xp, Yp)=h1G+h2KsG$を算出する。

【0152】ステップS117において、DSA署名生成・検証部72は、ステップS116の算出結果から、Pの値が無限遠点であるか否かを判断する。ここでは、Pの値が無限遠点である場合、ステップS116において、$h1G+h2KsG$の解を得ることができないことに基づいて、Pの値が無限遠点であるか否かを判断することが可能である。ステップS117において、Pが無限遠点であると判断された場合、処理は、ステップS120に進む。

【0153】ステップS117において、Pの値が無限遠点ではないと判断された場合、ステップS118において、DSA署名生成・検証部72は、$c=Xp \bmod r$が成り立つか否かを判断する。ステップS118において、$c=Xp \bmod r$が成り立たないと判断された場合、処理は、ステップS120に進む。

【0154】ステップS118において、$c=Xp \bmod r$が成り立つと判断された場合、ステップS119において、DSA署名生成・検証部72は、受信した署名は正しいと判断し、処理が終了される。

【0155】ステップS112において、$0<c<r$かつ$0<d<r$ではないと判断された場合、ステップS117において、pが無限遠点であると判断された場合、もしくは、ステップS118において、$c=Xp \bmod r$が成り立たないと判断された場合、ステップS120において、DSA署名生成・検証部72は、受信した署名は正しくないと判断し、処理が終了される。

【0156】また、図7(B)を用いて説明した認証用鍵情報を用いて認証鍵識別が行われ、あるサービスに対してレベル分けされた複数の認証鍵が格納されているような場合、低レベルの鍵から優先的に認証処理を開始し、その鍵のバージョンを判定し、その鍵のバージョンが古いとき、より高いレベルの認証鍵を用いて認証処理を行うようにしてもよい。

【0157】次に、図27のフローチャートを参照して、図15のステップS3において実行される、あるサービスに対してレベル分けされた複数の認証鍵が格納されている場合のリーダライタ2の認証鍵識別処理について説明する。

【0158】リーダライタ2の制御部101は、ステップS131において、通信部91を介して、鍵レベル交渉コマンドを、ICカード1に送信し、ステップS132において、後述する図28のステップS143において、ICカード1が送信する、レベルNにおける鍵バージョン情報Vを、通信部91を介して受信する。

【0159】ステップS133において、制御部101は、ステップS132において受信した鍵バージョン情報VのレベルNは、$N>0$であるか否かを判断する。ステップS133において、$N>0$ではないと判断された場合、処理はステップS137に進む。

【0160】ステップS133において、$N>0$であると判断された場合、ステップS134において、制御部101は、ステップS132において受信した鍵バージョン情報Vに基づいて、レベルNにおける鍵バージョン情報は有効か否かを判断する。

【0161】ステップS134において、レベルNにおける鍵バージョンが有効ではないと判断された場合(すなわち、鍵のバージョンが古いと判断された場合)、ステップS135において、制御部101は、通信部91を介して、ICカード1にNACK信号を送信し、処理はステップS132に戻り、それ以降の処理が繰り返される。

【0162】ステップS134において、レベルNにおける鍵バージョンは有効であると判断された場合、ステップS136において、制御部101は、通信部91を介して、ICカード1にACK信号を送信し、処理が終了される。

【0163】ステップS133において、$N>0$ではないと判断された場合、ステップS137において、図16のステップS16と同様の処理がなされ、処理が終了される。

【0164】次に、図28のフローチャートを参照して、図27を用いて説明したリーダライタ2の認証鍵識別処理と並行して実行される、ICカード1の認証鍵識別処理について説明する。なお、ここでも、図3を用いて説明したICカード1により、処理が実行される場合について説明するが、図4を用いて説明したICカード

1によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0165】ICカード1の制御部31は、ステップS141において、図27のステップS131において、リーダライタ2が送信した鍵レベル交渉コマンドを受信し、ステップS142において、現在の鍵レベルNを、N=1にセットする。

【0166】制御部31は、ステップS143において、現在の鍵レベルNと、そのレベルにおける鍵バージョン情報Vを、通信部21を介して、リーダライタ2に送信し、ステップS144において、図27のステップS135もしくはステップS136において、リーダライタ2が送信したデータを受信する。

【0167】ステップS145において、制御部31は、ステップS144において、リーダライタ2から受信した信号は、ACK信号であるか否かを判断する。ステップS145において、リーダライタ2から受信した信号はACK信号ではないと判断された場合、制御部31は、ステップS146において、N=N+1とし、ステップS147において、Nの値が所定の最大レベルを超えているか否かを判断する。

【0168】ステップS147において、Nが最大レベルを超えていないと判断された場合、処理はステップS143に戻り、それ以降の処理が繰り返される。ステップS147において、Nが最大レベルを超えていると判断された場合、ステップS148において、制御部31は、現在のレベルをN=0（N=0は、例外状態を示すものとする）とし、処理はステップS143に戻り、それ以降の処理が繰り返される。

【0169】ステップS145において、リーダライタ2から受信した信号はACK信号であると判断された場合、処理が終了される。

【0170】図15乃至図28を用いて、ICカード1と、リーダライタ2のサービス識別および認証鍵識別に関する処理について説明したが、例えば、図2を用いて説明したサービス登録用リーダライタ2-11に、ICカード1を装着し、新たなサービスの登録を実行する場合、およびサービスの削除を実行する場合には、図10を用いて説明したように、サービス登録用リーダライタ2-11のメモリ103に記憶されているサービス登録用の認証鍵Kregを用いて認証処理を行うため、図15乃至図28を用いて説明したような相互認証処理を用いなくてもよい。

【0171】次に、図29のフローチャートを参照して、サービス登録用リーダライタ2-11のサービス登録処理について説明する。

【0172】サービス登録用リーダライタ2-11の制御部101は、ステップS151において、通信部91を介して、サービス登録コマンドを、ICカード1に送信し、ステップS152において、ICカード1と、サービス登録用鍵Kregによる相互認証を行い、セッション鍵Ksesを共有する。

【0173】制御部101は、ステップS153において、空き領域確認コマンドを、通信部91を介してICカード1に送信し、ステップS154において、後述する図30のステップS175もしくはステップS176においてICカード1から送信されるデータを受信する。

【0174】ステップS155において、制御部101は、ステップS154において、ICカード1から受信した信号はACK信号であるか否かを判断する。ステップS155において、ICカード1から受信した信号がACK信号であると判断された場合、制御部101は、ステップS156において、暗号処理部102の共通鍵処理部112を制御して、ICカード1のメモリ32に新たに登録する登録データを、セッション鍵Ksesで暗号化させ、ステップS157において、暗号化データを、通信部91を介して、ICカード1に送信する。

【0175】制御部101は、ステップS158において、後述する図30のステップS180において、ICカード1が送信したデータ登録完了通知を、通信部91を介して受信し、ステップS159において、サービス認証によるサービス削除許可フラグを送信し、処理が終了される。

【0176】ステップS155において、ICカード1から受信した信号がACK信号ではないと判断された場合、ステップS160において、図16のステップS16と同様の処理がなされ、処理が終了される。

【0177】次に、図30のフローチャートを参照して、図29を用いて説明した、サービス登録用リーダライタ2-11のサービス登録処理と並行して実行される、ICカード1のサービス登録処理について説明する。なお、ここでも、図3を用いて説明したICカード1により、処理が実行される場合について説明するが、図4を用いて説明したICカード1によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0178】ステップS171において、ICカード1の制御部31は、通信部21を介して、図29のステップS151において、サービス登録用リーダライタ2-11が送信したサービス登録コマンドを受信する。

【0179】制御部31は、ステップS172において、ICカード1と、サービス登録用鍵Kregによる相互認証を行い、セッション鍵Ksesを共有し、ステップS173において、通信部21を介して、図29のステップS153において、サービス登録用リーダライタ2-11が送信した、空き領域確認コマンドを受信する。

【0180】ステップS174において、制御部31は、メモリ32のSRA46に、登録データ用の空き領域があるか否かを判断する。ステップS174におい

て、空き領域がないと判断された場合、ステップS175において、制御部31は、サービス登録用リーダライタ2-11に、通信部21を介して、NACK信号を送信し、処理が終了される。

【0181】ステップS174において、空き領域があると判断された場合、ステップS176において、制御部31は、サービス登録用リーダライタ2-11に、通信部21を介して、ACK信号を送信する。

【0182】制御部31は、ステップS177において、図29のステップS157において、サービス登録用リーダライタ2-11が送信した暗号化データを、通信部21を介して受信し、ステップS178において、暗号処理部33の共通鍵処理部42を制御して、ステップS177において受信した暗号化データを、セッション鍵Ksesを用いて復号させる。

【0183】ステップS179において、制御部31は、ステップS178において、セッション鍵Ksesにより復号されたデータを、メモリ32に供給し、SRA46のService Individual Info領域およびSRT45に登録させる。

【0184】制御部31は、ステップS180において、データの登録完了を、通信部21を介して、サービス登録用リーダライタ2-11に通知し、ステップS181において、図29のステップS159において、サービス登録用リーダライタ2-11が送信した、サービス認証によるサービス削除許可フラグを受信し、サービス削除許可フラグを、メモリ32のSRA46のService Individual Info領域に設定し、処理が終了される。

【0185】次に、図31のフローチャートを参照して、サービス登録用リーダライタ2-11のサービス削除処理について説明する。

【0186】ステップS191において、サービス登録用リーダライタ2-11の制御部101は、ユーザが、入力部106を用いて入力した、削除するサービスに対応するサービスIDの入力を受ける（ここでは、対応するサービスIDが、ID_Sであるサービスが削除されるものとする）。

【0187】ステップS192において、図29のステップS152と同様の処理がなされる。制御部101は、ステップS193において、通信部91を介して、ICカード1に、ID_S領域削除コマンドを送信し、ステップS194において、後述する図32のステップS205においてICカード1が送信した、エラーメッセージを受信したか否かを判断する。

【0188】ステップS194において、エラーメッセージを受信したと判断された場合、ステップS195において、図16のステップS16と同様の処理がなされ、処理が終了される。ステップS194において、エラーメッセージを受信しなかったと判断された場合、処理が終了される。

【0189】次に、図32のフローチャートを参照して、図31を用いて説明した、サービス登録用リーダライタ2-11のサービス削除処理と並行して実行される、ICカード1のサービス削除処理について説明する。なお、ここでも、図3を用いて説明したICカード1により、処理が実行される場合について説明するが、図4を用いて説明したICカード1によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0190】ステップS201において、図30のステップS172と同様の処理が実行される。ICカード1の制御部31は、ステップS202において、図31のステップS193において、サービス登録用リーダライタ2-11が送信した、ID_S領域削除コマンドを受信し、ステップS203において、ID_S領域に対応するデータがあるか否かを確認することなどにより、ステップS202において受信したID_S領域削除コマンドの正当性が検証されたか否かを判断する。

【0191】ステップS203において、ID_S領域削除コマンドの正当性が検証されたと判断された場合、ステップS204において、制御部31は、メモリ32のSRT45およびSRA46から、ID_Sに対応する領域を削除し、処理が終了される。

【0192】ステップS203において、ID_S領域削除コマンドの正当性が検証されなかったと判断された場合、ステップS205において、制御部31は、通信部21を介して、サービス登録用リーダライタ2-11に、エラーメッセージを送信し、処理が終了される。

【0193】図31および図32を用いて説明したサービス削除処理は、一般リーダライタ2-12とICカード1とで実行することも可能である。図33のフローチャートを参照して、一般リーダライタ2-12のサービス削除処理について説明する。

【0194】ステップS211において、図16、もしくは図18を用いて説明した、リーダライタ2のサービス識別処理が実行され、ステップS212において、図20、図22、もしくは図27を用いて説明したリーダライタ2の認証鍵識別処理が実行され、ステップS213において、図31のステップS193と同様の処理が実行される。

【0195】ステップS214において、一般リーダライタ2-12の制御部101は、後述する図34のステップS226もしくはステップS227において、ICカード1が送信する信号を受信する。そして、ステップS215およびステップS216において、図16のステップS15およびステップS16と同様の処理が実行され、処理が終了される。

【0196】次に、図34のフローチャートを参照して、図33を用いて説明した、一般リーダライタ2-12のサービス削除処理と並行して実行される、ICカー

ド１のサービス削除処理について説明する。なお、ここでも、図３を用いて説明したＩＣカード１により、処理が実行される場合について説明するが、図４を用いて説明したＩＣカード１によって処理が実行される場合においても、基本的に同様の処理が実行される。

【０１９７】ステップＳ２２１において、図１７、もしくは図１９を用いて説明した、ＩＣカード１のサービス識別処理が実行され、ステップＳ２３２において、図２１、図２３、もしくは図２８を用いて説明したＩＣカード１の認証鍵識別処理が実行される。

【０１９８】ステップＳ２２３において、制御部３１は、図３３のステップＳ２１３において、一般リーダライタ２－１２が送信した、ＩＤ_Ｓ領域削除コマンドを、通信部２１を介して受信する。ステップＳ２２４において、図３２のステップＳ２０３と同様の処理が実行される。ステップＳ２２４において、コマンドの正当性が検証されたと判断された場合、ステップＳ２２５において、図３２のステップＳ２０４と同様の処理がなされ、ステップＳ２２６において、制御部３１は、通信部２１を介して、一般リーダライタ２－１２にＡＣＫ信号を送信し、処理が終了される。

【０１９９】ステップＳ２２４において、コマンドの正当性が検証されなかったと判断された場合、ステップＳ２２７において、制御部３１は、通信部２１を介して、一般リーダライタ２－１２にＮＡＣＫ信号を送信し、処理が終了される。

【０２００】次に、図３５のフローチャートを参照して、ユーザが、一般リーダライタ２－１２で、ＩＣカード１に登録されているサービスを受ける場合に実行される、一般リーダライタ２－１２のサービス取得処理について説明する。

【０２０１】ステップＳ２３１において、図１６、もしくは図１８を用いて説明した、リーダライタ２のサービス識別処理が実行され、ステップＳ２３２において、図２０、図２２、もしくは図２７を用いて説明したリーダライタ２の認証鍵識別処理が実行される。

【０２０２】ステップＳ２３３において、一般リーダライタ２－１２の制御部１０１は、通信部９１を介して、ＩＣカード１に、ＩＤ_Ｓ領域のデータ要求コマンドを送信する。

【０２０３】制御部１０１は、ステップＳ２３４において、後述する図３６のステップＳ２４５において、ＩＣカード１から送信されるデータを受信し、ステップＳ２３５において、暗号処理部１０２の共通鍵処理部１１２を制御して、ステップＳ２３４において受信した暗号化データを、セッション鍵Ksesを用いて復号させる。制御部１０１は、復号されたデータを用いて、例えば、電子マネーの減算や加算などの所定のデータ処理を行い、処理が終了される。

【０２０４】次に、図３６のフローチャートを参照して、図３５を用いて説明した、一般リーダライタ２－１２のサービスデータ取得処理と並行して実行される、ＩＣカード１のサービスデータ取得処理について説明する。なお、ここでも、図３を用いて説明したＩＣカード１により、処理が実行される場合について説明するが、図４を用いて説明したＩＣカード１によって処理が実行される場合においても、基本的に同様の処理が実行される。

【０２０５】ステップＳ２４１において、図１７、もしくは図１９を用いて説明した、ＩＣカード１のサービス識別処理が実行され、ステップＳ２３２において、図２１、図２３、もしくは図２８を用いて説明したＩＣカード１の認証鍵識別処理が実行される。

【０２０６】ステップＳ２４３において、ＩＣカード１の制御部３１は、通信部２１を介して、図３５のステップＳ２３３において、一般リーダライタ２－１２が送信した、ＩＤ_Ｓ領域のデータ要求コマンドを受信する。制御部３１は、ステップＳ２４４において、暗号処理部３３の共通鍵処理部４２を制御して、メモリ３２のＩＤ_Ｓに対応する領域に登録しているデータを、セッション鍵Ksesを用いて暗号化させ、ステップＳ２４５において、通信部２１を介して、暗号化したデータを一般リーダライタ２－１２に送信し、処理が終了される。

【０２０７】また、ＩＣカード１と一般リーダライタ２－１２において、あるサービスに関する情報の授受がなされている場合においても、図８を用いて説明したＳＲＴ４５に、対応するパーミッション情報が記録されている場合、現在情報の授受がなされている以外のサービスに関する情報の授受を行うことが可能である。図３７のフローチャートを参照して、ＩＤ_Ｓ以外のサービスＩＤに対応するサービスの実行中に行われる、一般リーダライタ２－１２のサービスデータ取得処理について説明する。

【０２０８】ステップＳ２５１乃至ステップＳ２５４において、図３５のステップＳ２３１乃至ステップＳ２３４と同様の処理が実行される。ステップＳ２５５において、一般リーダライタ２－１２の制御部１０１は、ステップＳ２５４において、ＩＣカード１から受信したデータは、ＮＡＣＫ信号か否かを判断する。

【０２０９】ステップＳ２５５において、受信したデータがＮＡＣＫ信号ではないと判断された場合、ステップＳ２５６において、図３５のステップＳ２３５と同様の処理が実行され、処理が終了される。ステップＳ２５５において、受信したデータがＮＡＣＫ信号であると判断された場合、図１６のステップＳ１６と同様の処理がなされ、処理が終了される。

【０２１０】次に、図３８のフローチャートを参照して、図３７を用いて説明した、一般リーダライタ２－１２のサービスデータ取得処理と並行して実行される、ＩＣカード１のサービスデータ取得処理について説明す

る。なお、ここでも、図3を用いて説明したICカード1により、処理が実行される場合について説明するが、図4を用いて説明したICカード1によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0211】ステップS261乃至ステップS263において、図34のステップS241乃至ステップS243と同様の処理が実行される。なお、ステップS261では、サービスID_Sとは異なる、サービスID_Tの認証が行われるものとする。ステップS264において、ICカード1の制御部31は、メモリ32のSRT45およびSRA46に、ステップS263において受信したデータ要求コマンドに対応するID_S領域が登録されているか否かを判断する。ステップS264において、ID_S領域が登録されていないと判断された場合、処理は、ステップS269に進む。

【0212】ステップS264において、ID_S領域が登録されていると判断された場合、制御部31は、ステップS265において、メモリ32のSRT45の、ID_Sに対応するパーミッション情報フィールドから、ID_Sのパーミッション情報を取得し、ステップS266において、ID_T認証時に、ID_Sのデータの読み込みが許可されているか否かを判断する（すなわち、SRT45のID_Sに対応するパーミッション情報フィールドに、ID_Tによる認証時に、データの読み出し許可、すなわち、roもしくはrwが記載されているか否かを判断する）。ステップS266において、データの読み込みが許可されていないと判断された場合、処理はステップS269に進む。

【0213】ステップS266において、データの読み込みが許可されていると判断された場合、ステップS267およびステップS268において、図36のステップS244およびステップS245と同様の処理が実行され、処理が終了される。

【0214】ステップS264において、ID_S領域が登録されていないと判断された場合、もしくは、ステップS266において、データの読み込みが許可されていないと判断された場合、ステップS269において、制御部31は、通信部21を介して、一般リーダライタ2－12にNACK信号を送信し、処理が終了される。

【0215】図35乃至図48を用いて説明したサービスデータ取得処理によって、ICカード1から一般リーダライタ2－12にデータが取得され、所定の処理がなされたあと、一般リーダライタ2－12は、必要に応じて、ICカード1のメモリ32のSRT45もしくはSRA46の所定の領域に対して、データを書き込む処理を実行する。

【0216】次に、図39のフローチャートを参照して、一般リーダライタ2－12のサービスデータ書き込み処理について説明する。

【0217】ステップS281において、図16、もしくは図18を用いて説明した、リーダライタ2のサービス識別処理が実行され、ステップS282において、図20、図22、もしくは図27を用いて説明したリーダライタ2の認証鍵識別処理が実行される。

【0218】一般リーダライタ2－12の制御部101は、ステップS283において、ICカード1のメモリ32に書き込むために、ICカード1に送信するデータを、暗号処理部102の共通鍵処理部112を制御して、セッション鍵Ksesを用いて暗号化させ、ステップS284において、ICカード1に、データ書き込みコマンドと、ステップS284において暗号化したデータを、通信部91を介して送信し、処理が終了される。

【0219】次に、図40のフローチャートを参照して、図39を用いて説明した、一般リーダライタ2－12のサービスデータ書き込み処理と並行して実行される、ICカード1のサービスデータ書き込み処理について説明する。なお、ここでも、図3を用いて説明したICカード1により、処理が実行される場合について説明するが、図4を用いて説明したICカード1によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0220】ステップS291において、図17、もしくは図19を用いて説明した、ICカード1のサービス識別処理が実行され、ステップS232において、図21、図23、もしくは図28を用いて説明したICカード1の認証鍵識別処理が実行される。

【0221】ステップS293において、制御部31は、通信部21を介して、図39のステップS284において、一般リーダライタ2－12が送信した、データ書き込みコマンドと暗号化データを受信する。制御部31は、ステップS294において、暗号処理部33の共通鍵処理部42を制御して、受信したデータを、セッション鍵Ksesを用いて復号させ、ステップS295において、復号したデータを、メモリ32のSRT45およびSRA46のID_Sに対応するサービス格納領域へ書き込み、処理が終了される。

【0222】また、ICカード1と一般リーダライタ2－12において、あるサービスに関する情報の授受がなされている場合においても、図8を用いて説明したSRT45に、対応するパーミッション情報が記録されている場合、図37および図38を用いて説明したサービスデータ取得処理と同様に、現在情報の授受がなされている以外のサービスに関するサービスデータ書き込み処理を実行することが可能である。図41のフローチャートを参照して、ID_S以外のサービスIDに対応するサービスの実行中に行われる、一般リーダライタ2－12のサービスデータ書き込み処理について説明する。

【0223】ステップS301乃至ステップS304において、図39のステップS281乃至ステップS28

4と同様の処理が実行される。そして、ステップS305およびステップS306において、図16のステップS15およびステップS16と同様の処理がなされ、処理が終了される。

【0224】次に、図42のフローチャートを参照して、図41を用いて説明した、一般リーダライタ2-12のサービスデータ書き込み処理と並行して実行される、ICカード1のサービスデータ書き込み処理について説明する。なお、ここでも、図3を用いて説明したICカード1により、処理が実行される場合について説明するが、図4を用いて説明したICカード1によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0225】ステップS311乃至ステップS313において、図40のステップS291乃至ステップS293と同様の処理が実行される。なお、ステップS311では、サービスID_Sとは異なる、サービスID_Tの認証が行われるものとする。ステップS314およびステップS315において、図38のステップS264およびステップS265と同様の処理がなされ、ステップS314において、ID_S領域が登録されていないと判断された場合、処理は、ステップS320に進む。

【0226】ステップS316において、制御部31は、ID_T認証時に、ID_Sのサービスに対して、データの書き込みが許可されているか否かを判断する（すなわち、SRT45のID_Sに対応するパーミッション情報フィールドに、ID_T認証時のデータの書き込み許可、すなわち、rwが記載されているか否かを判断する）。ステップS316において、データの書き込みが許可されていないと判断された場合、処理はステップS320に進む。

【0227】ステップS316において、データの書き込みが許可されていると判断された場合、ステップS317およびステップS318において、図40のステップS294およびステップS295と同様の処理が実行される。ステップS319において、制御部31は、通信部21を介して、一般リーダライタ2-12にACK信号を送信し、処理が終了される。

【0228】ステップS314において、ID_S領域が登録されていないと判断された場合、もしくは、ステップS316において、データの書き込みが許可されていないと判断された場合、ステップS320において、制御部31は、通信部21を介して、一般リーダライタ2-12にNACK信号を送信し、処理が終了される。

【0229】以上説明したように、一般リーダライタ2-12に、ICカード1を装着し、各種サービスを受けるためには、サービス毎に定められた共通鍵、もしくは公開鍵を用いて認証処理を行わなければならない。これらの認証鍵は、セキュリティの維持のために、しばしばバージョンアップされる（すなわち、鍵が変更される）。ユーザは、図2を用いて説明したバージョンアップ用リーダライタ2-14、もしくは一般リーダライタ2-12に、ICカード1を装着し、図43乃至図47を用いて後述する鍵バージョンアップ処理を実行させることにより、自分自身が管理しているICカード1に登録されている認証鍵を、できるだけ最新に近いバージョンの認証鍵にバージョンアップするようにしなければならない。

【0230】次に、図43を参照して、サービス毎に定められたバージョンアップ用鍵（図6および図14を用いて説明したバージョンアップ用鍵Kake_vup）を用いて実行される、バージョンアップ用リーダライタ2-14の鍵バージョンアップ処理について説明する。

【0231】ステップS331において、図16、もしくは図18を用いて説明した、リーダライタ2のサービス識別処理が実行され、ステップS332において、図20、図22、もしくは図27を用いて説明したリーダライタ2の認証鍵識別処理が実行される。

【0232】ステップS333において、バージョンアップ用リーダライタ2-14の制御部101は、暗号処理部102の共通鍵処理部112を制御して、バージョンアップを行う認証鍵に対応する認証鍵IDを、セッション鍵Ksesを用いて暗号化させ、ICカード1に送信する。ステップS334において、制御部101は、後述する図44のステップS355もしくはステップS360において、ICカード1が送信する信号を受信する。

【0233】ステップS335において、制御部101は、ステップS334においてICカード1から受信した信号はACK信号であるか否かを判断する。ステップS335において、受信した信号がACK信号ではないと判断された場合、処理は、ステップS339に進む。ステップS335において、受信した信号がACK信号であると判断された場合、ステップS336において、制御部101は、バージョンアップを行う認証鍵に対応する最新バージョン情報と、認証鍵Kakeをメモリ103から読み出し、暗号処理部102の共通鍵処理部112を制御して、セッション鍵Ksesを用いて暗号化させ、通信部91を介して、ICカード1に送信する。

【0234】そして、ステップS337において、ICカード1が、後述する44のステップS359もしくはステップS360において送信した信号を受信する。ステップS338において、ステップS335と同様の処理がなされ、ステップS338において、受信した信号がACK信号であると判断された場合、処理が終了される。ステップS335およびステップS338において、受信した信号がACK信号ではないと判断された場合、ステップS339において、図16のステップS16と同様の処理がなされ、処理が終了される

【0235】次に、図44のフローチャートを参照して、図43を用いて説明した、バージョンアップ用リー

ダライタ2－14の鍵バージョンアップ処理と並行して実行される、ICカード1の鍵バージョンアップ処理について説明する。なお、ここでも、図3を用いて説明したICカード1により、処理が実行される場合について説明するが、図4を用いて説明したICカード1によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0236】ステップS351において、図17、もしくは図19を用いて説明した、ICカード1のサービス識別処理が実行され、ステップS352において、図21、図23、もしくは図28を用いて説明したICカード1の認証鍵識別処理が実行される。

【0237】ステップS353において、制御部31は、通信部21を介して、図43のステップS333において、バージョンアップ用リーダライタ2－14が送信した、暗号化された認証鍵IDを受信し、暗号処理部33の共通鍵処理部42を制御して、受信したデータを、セッション鍵Ksesを用いて復号させる。ステップS354において、制御部31は、復号したデータを基に、メモリ32のSRT45およびSRA46のID_Sに、対応する認証鍵IDが存在するか否かを判断する。ステップS354において、認証鍵IDが存在しないと判断された場合、処理は、ステップS360に進む。

【0238】ステップS354において、認証鍵IDが存在すると判断された場合、制御部31は、ステップS355において、通信部21を介して、バージョンアップ用リーダライタ2－14に、ACK信号を送信し、ステップS356において、図43のステップS336において、バージョンアップ用リーダライタ2－14が送信した、暗号化された最新バージョン情報と認証鍵Kakeを、通信部21を介して受信し、暗号処理部33の共通鍵処理部42を制御して、受信したバージョン情報を、セッション鍵Ksesを用いて復号させる。

【0239】ステップS357において、制御部31は、復号したデータを基に、受信したバージョン情報は正しいか否か（すなわち、自分自身がすでに保有している認証鍵のバージョン情報より新しいバージョンであるか否か）を判断する。ステップS357において、バージョン情報が正しくないと判断された場合、処理は、ステップS360に進む。

【0240】ステップS357において、バージョン情報は正しいと判断された場合、制御部31は、暗号処理部33の共通鍵処理部42を制御して、認証鍵Kakeを、セッション鍵Ksesを用いて復号させ、メモリ32のSRA46における、認証鍵Kakeが記載される領域に書き込み、ステップS359において、バージョンアップ用リーダライタ2－14に、通信部21を介してACK信号を送信し、処理が終了される。

【0241】ステップS354において、認証鍵IDが存在しないと判断された場合、およびステップS357において、バージョン情報が正しくないと判断された場合、ステップS360において、制御部31は、バージョンアップ用リーダライタ2－14に、通信部21を介してNACK信号を送信し、処理が終了される。

【0242】また、ICカード1と一般リーダライタ2－12において、あるサービスに関する情報の授受がなされている場合において、図8を用いて説明したSRT45に、対応するパーミッション情報が記録されている場合、図37および図38を用いて説明したサービスデータ取得処理や、図41および図42を用いて説明したサービスデータ書き込み処理と同様に、現在情報の授受がなされている以外のサービスに関する鍵バージョンアップ処理を実行することが可能である。図45のフローチャートを参照して、ID_S以外のサービスIDに対応するサービスの実行中に行われる、一般リーダライタ2－12の鍵バージョンアップ処理について説明する。

【0243】ステップS371およびステップS372において、図44のステップS331およびステップS332と同様の処理が実行される。そして、一般リーダライタ2－12の制御部101は、ステップS373において、ID_Sに対応するサービスの認証鍵のバージョンアップコマンドを、通信部91を介してICカード1に送信し、ステップS374において、後述する図46のステップS397もしくは図47のステップS405において、ICカード1が送信するデータを受信し、ステップS375において、ICカード1から受信した信号は、ACK信号か否かを判断する。

【0244】ステップS375において、受信した信号がACK信号でないと判断された場合、処理は、ステップS382に進む。ステップS375において、受信した信号がACK信号であると判断された場合、ステップS376乃至ステップS382において、図43のステップS333乃至ステップS339と同様の処理がなされ、処理が終了される。

【0245】次に、図46および図47のフローチャートを参照して、図45を用いて説明した、バージョンアップ用リーダライタ2－14の鍵バージョンアップ処理と並行して実行される、ICカード1の鍵バージョンアップ処理について説明する。なお、ここでも、図3を用いて説明したICカード1により、処理が実行される場合について説明するが、図4を用いて説明したICカード1によって処理が実行される場合においても、基本的に同様の処理が実行される。

【0246】ステップS391およびステップS392において、図44のステップS351およびステップS352と同様の処理が実行される。なお、ステップS391では、サービスID_Sとは異なる、サービスID_Tの認証が行われるものとする。ステップS393において、制御部31は、図45のステップS373におい

て、バージョンアップ用リーダライタ２－１４が送信した、ＩＤ_Ｓの認証鍵のバージョンアップコマンドを受信する。

【０２４７】ステップＳ３９４およびステップＳ３９５において、図３８のステップＳ２６４およびステップＳ２６５と同様の処理がなされ、ステップＳ３９４において、ＩＤ_Ｓ領域が登録されていないと判断された場合、処理は、ステップＳ４０５に進む。

【０２４８】ステップＳ３９６において、制御部３１は、ＩＤ_Ｔ認証時に、ＩＤ_Ｓの認証鍵のバージョンアップが許可されているか否かを判断する（すなわち、ＳＲＴ４５のＩＤ_Ｓに対応するパーミッション情報フィールドに、ＩＤ_Ｔ認証時のｖｕｐの許可が記載されているか否かを判断する）。ステップＳ３９６において、認証鍵のバージョンアップが許可されていないと判断された場合、処理は、ステップＳ４０５に進む。

【０２４９】ステップＳ３９６において、認証鍵のバージョンアップが許可されていると判断された場合、ステップＳ３９７において、制御部３１は、通信部２１を介して、バージョンアップ用リーダライタ２－１４に、ＡＣＫ信号を送信する。

【０２５０】そして、ステップＳ３９８乃至ステップＳ４０５において、図４４のステップＳ３５３乃至ステップＳ３６０と同様の処理が実行され、処理が終了される。

【０２５１】次に、図４８乃至図５１のフローチャートを参照して、図１３を用いて説明したモジュール間通信について説明する。モジュール間通信は、図４を用いて説明したＩＣカード１と、モジュール間通信用リーダライタ２－１３によって実行される。ここでは、図４を用いて説明したＩＣカード１の通信部５１および共通鍵サービス処理部５２を、図１３を用いて説明した共通鍵モジュール１２２とし、図４を用いて説明した通信部５３および公開鍵サービス処理部５４を、図１３を用いて説明した公開鍵モジュール１２１として説明する。

【０２５２】まず、図４８のフローチャートを参照して、共通鍵モジュール１２２が、モジュール間通信用リーダライタ２－１３と共有するセッション鍵と、公開鍵モジュール１２１が、モジュール間通信用リーダライタ２－１３と共有するセッション鍵とが異なる場合におけるモジュール間通信について説明する。

【０２５３】ステップＳ４１１において、モジュール間通信用リーダライタ２－１３は、図１６、もしくは図１８を用いて説明した、リーダライタ２のサービス識別処理を実行し、ステップＳ４１２において、ＩＣカード１の公開鍵モジュール１２１は、図１７、もしくは図１９を用いて説明した、ＩＣカード１のサービス識別処理を実行し、モジュール間リーダライタ２－１３と、公開鍵モジュール１２１の間で、セッション鍵Ｋses１を共有する。

【０２５４】ステップＳ４１３において、モジュール間通信用リーダライタ２－１３は、図１６、もしくは図１８を用いて説明した、リーダライタ２のサービス識別処理を実行し、ステップＳ４１４において、ＩＣカード１の共通鍵モジュール１２２は、図１７、もしくは図１９を用いて説明した、ＩＣカード１のサービス識別処理を実行し、モジュール間リーダライタ２－１３と、共通鍵モジュール１２２の間で、セッション鍵Ｋses２を共有する。

【０２５５】ステップＳ４１５において、モジュール間通信用リーダライタ２－１３の制御部１０１は、ステップＳ４１１およびステップＳ４１３において実行されたリーダライタ２のサービス識別処理において得られたＩＣカード１のカードＩＤを基に、公開鍵モジュール１２１と、共通鍵モジュール１２２の２つのカードＩＤが一致したか否かを判断する。ステップＳ４１５において、カードＩＤが一致しないと判断された場合、ステップＳ４１６において、図１６のステップＳ１６と同様の処理が実行される。

【０２５６】ステップＳ４１５において、２つのカードＩＤが一致すると判断された場合、ステップＳ４１７において、モジュール間通信用リーダライタ２－１３の制御部１０１は、モジュールデータ移動コマンドを公開鍵モジュール１２１に送信する。

【０２５７】公開鍵モジュール１２１の制御部６１は、ステップＳ４１８において、モジュールデータ移動開始コマンドをモジュール間通信用リーダライタ２－１３から受信し、暗号処理部３３の、共通鍵処理部４２を制御して、移動するデータをセッション鍵Ｋses１で暗号化させ、ステップＳ４１９で、暗号化データをモジュール間通信用リーダライタ２－１３に送信する。

【０２５８】モジュール間通信用リーダライタ２－１３の制御部１０１は、ステップＳ４２０において、暗号処理部１０２の、共通鍵処理部１１２を制御して、受信したデータをセッション鍵Ｋses１で復号し、ステップＳ４２１において、データをセッション鍵Ｋses２で暗号化させ、共通鍵モジュール１２２に送信する。共通鍵モジュール１２２の制御部６１は、ステップＳ４２２において、暗号処理部６３の、共通鍵処理部４２を制御して、受信したデータをセッション鍵Ｋses２で復号させ、ステップＳ４２３において、復号したデータをメモリ６２の対応する領域に保存して利用する。

【０２５９】次に、図４９のフローチャートを参照して、共通鍵モジュール１２２が、モジュール間通信用リーダライタ２－１３と共有するセッション鍵と、公開鍵モジュール１２１が、モジュール間通信用リーダライタ２－１３と共有するセッション鍵とが同一である場合におけるモジュール間通信について説明する。

【０２６０】ステップＳ４３１において、モジュール間通信用リーダライタ２－１３は、図１６、もしくは図１

８を用いて説明した、リーダライタ２のサービス識別処理を実行し、ステップＳ４３２において、ＩＣカード１の公開鍵モジュール１２１は、図１７、もしくは図１９を用いて説明した、ＩＣカード１のサービス識別処理を実行し、モジュール間リーダライタ２－１３と、公開鍵モジュール１２１の間で、セッション鍵Kses１を共有する。

【０２６１】ステップＳ４３３において、モジュール間通信用リーダライタ２－１３は、図１６、もしくは図１８を用いて説明した、リーダライタ２のサービス識別処理を実行し、ステップＳ４３４において、ＩＣカード１の共通鍵モジュール１２２は、図１７、もしくは図１９を用いて説明した、ＩＣカード１のサービス識別処理を実行し、モジュール間リーダライタ２－１３と、共通鍵モジュール１２２の間で、セッション鍵Kses１を共有する。

【０２６２】ステップＳ４３５乃至ステップＳ４３９において、図４８のステップＳ４１５乃至ステップＳ４１９と同様の処理が実行される。そして、ステップＳ４４０において、モジュール間通信用リーダライタ２－１３の制御部１０１は、受信したデータを、共通鍵モジュール１２２に送信する。図４８のステップＳ４２０およびステップＳ４２１においては、受信したデータをセッション鍵Kses１で復号し、復号したデータをセッション鍵Kses２で暗号化した後に共通鍵モジュール１２２に送信したが、ここでは、共通鍵モジュール１２２も、セッション鍵Kses１を有しているため、これらの処理が必要なくなる。

【０２６３】共通鍵モジュール１２２の制御部６１は、ステップＳ４１１において、暗号処理部６３を制御して、受信したデータをセッション鍵Kses１で復号し、ステップＳ４２２において、復号したデータをメモリ６２の対応する領域に保存して利用する。

【０２６４】次に、図５０のフローチャートを参照して、共通鍵モジュール１２２が、モジュール間通信用リーダライタ２－１３と共有するセッション鍵と、公開鍵モジュール１２１が、モジュール間通信用リーダライタ２－１３と共有するセッション鍵とが異なるが、モジュール間通信用リーダライタ２－１３が、共通鍵モジュール１２２が有するセッション鍵を、公開鍵モジュール１２１が有するもう一方のセッション鍵で暗号化し、公開鍵モジュール１２１に供給するようになされている場合におけるモジュール間通信について説明する。

【０２６５】ステップＳ４５１乃至ステップＳ４５６において、図４８のステップＳ４１１乃至ステップＳ４１６と同様の処理が実行される。すなわち、モジュール間リーダライタ２－１３と、公開鍵モジュール１２１の間で、セッション鍵Kses１が共有され、モジュール間リーダライタ２－１３と、共通鍵モジュール１２２の間で、セッション鍵Kses２が共有される。

【０２６６】ステップＳ４５７において、モジュール間通信用リーダライタ２－１３の制御部１０１は、暗号処理部１０２を制御して、セッション鍵Kses２を、セッション鍵Kses１で暗号化させ、公開鍵モジュール１２１に送信する。公開鍵モジュール１２１の制御部６１は、暗号処理部３３の共通鍵処理部４２を制御して、受信したデータをセッション鍵Kses１で復号させることにより、セッション鍵Kses２を取り出す。

【０２６７】ステップＳ４５９において、図４８のステップＳ４１７と同様の処理が実行される。ステップＳ４６０において、公開鍵モジュール１２１の制御部６１は、移動するデータをセッション鍵Kses２で暗号化し、暗号化データをモジュール間通信用リーダライタ２－１３に送信する。

【０２６８】ステップＳ４６１において、図４９のステップＳ４４０と同様の処理が実行される。そして、ステップＳ４６２およびステップＳ４６３において、図４８のステップＳ４２２およびＳ４２３と同様の処理が実行される。

【０２６９】すなわち、図４８のステップＳ４２０およびステップＳ４２１においては、受信したデータをセッション鍵Kses１で復号し、復号したデータをセッション鍵Kses２で暗号化した後に共通鍵モジュール１２２に送信したが、ここでは、図４９を用いて説明した処理と同様に、共通鍵モジュール１２２と、公開鍵モジュール１２１とが、同一のセッション鍵Kses２を得ることができるため、これらの処理を行う必要がない。

【０２７０】そして、図５１のフローチャートを参照して、公開鍵モジュール１２１と共通鍵モジュール１２２が、共通秘密鍵K_commonを共有し、それを用いて相互認証を行い、更に、共通のセッション鍵Ksesを共有する場合の、モジュール間通信について説明する。

【０２７１】ステップＳ４７１およびステップＳ４７２において、公開鍵モジュール１２１と共通鍵モジュール１２２は、共通秘密鍵K_commonにより、相互認証を行い、セッション鍵Ksesを共有する。ステップＳ４７３において、モジュール間通信用リーダライタ２－１３は、ステップＳ４７１およびステップＳ４７２における相互認証の通信路のみ提供する（すなわち、公開鍵モジュール１２１とも共通鍵モジュール１２２とも、セッション鍵の共有は行われない）。

【０２７２】ステップＳ４７４において、図４８のステップＳ４１７と同様の処理が実行される。ステップＳ４７５において、公開鍵モジュール１２１の制御部６１は、暗号処理部３３の共通鍵処理部４２を制御して、移動するデータをセッション鍵Ksesで暗号化させ、暗号化データをモジュール間通信用リーダライタ２－１３に送信する。そして、ステップＳ４７６乃至ステップＳ４７８において、図４９のステップＳ４２１乃至ステップＳ４２３と同様の処理が実行される。

【0273】すなわち、図51を用いて説明したモジュール間通信においては、モジュール間通信用リーダライタ2-13は、データの通信路を提供するのみで、モジュール間通信されるデータを暗号化したり、復号することはない。

【0274】上述した一連の処理は、ソフトウェアにより実行することもできる。そのソフトウェアは、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば汎用のパーソナルコンピュータなどに、記録媒体からインストールされる。

【0275】この記録媒体は、図9に示すように、コンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク115（フロッピー（登録商標）ディスクを含む）、光ディスク116（CD-ROM(Compact Disk-Read Only Memory)，DVD(Digital Versatile Disk)を含む）、光磁気ディスク117（MD(Mini-Disk)を含む）、もしくは半導体メモリ118などよりなるパッケージメディアなどにより構成される。

【0276】また、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

【0277】

【発明の効果】本発明の第1のデータ記憶装置、データ記憶方法、および記録媒体に記録されているプログラムによれば、情報処理装置に対する、データの入出力を制御し、秘密情報の記憶を制御し、記憶された秘密情報のうちの第1の秘密情報のバージョン情報と、入力された第2の秘密情報のバージョン情報より、第1の秘密情報のバージョンと、第2の秘密情報のバージョンを比較し、第2の秘密情報のほうが、第1の秘密情報よりもバージョンが新しいと判断された場合、第1の秘密情報を記憶していた記憶領域へ第2の秘密情報を記憶させるように制御するようにしたので、ICカードとリーダライタとの相互認証に用いられる認証鍵などの、秘密情報のアップデートを、通常のサービスデータの授受とは異なるモードでのICカードとリーダライタ間の通信によって可能とすることができる。

【0278】本発明の第2のデータ記憶装置、データ記憶方法、および記録媒体に記録されているプログラムによれば、情報処理装置に対する、データの入出力を制御し、所定のサービスに対応するデータおよび情報処理装置との認証処理に用いられる複数の認証鍵の記憶を制御し、記憶された複数の認証鍵から情報処理装置との認証処理に用いられる認証鍵を選択し、選択された認証鍵を用いて認証処理を行い、選択された第1の認証鍵による認証処理が行えなかった場合、第1の認証鍵と異なる第2の認証鍵をさらに選択するようにしたので、ある認証鍵が第3者に漏洩してしまった場合などに、使用することができなくなった認証鍵以外の他の認証鍵を用いて、認証処理を実行することを可能とすることができる。

【0279】本発明の第1の情報処理装置、情報処理方法、および記録媒体に記録されているプログラムによれば、データ記憶装置に対する、データの入出力を制御し、複数の秘密情報の記憶を制御し、ユーザによる秘密情報の選択を示す信号の入力を制御し、入力された秘密情報の選択を示す信号に基づいて、記憶された複数の秘密情報から所定の秘密情報を選択し、選択された秘密情報および秘密情報のバージョン情報の、データ記憶装置への出力を制御するようにしたので、ICカードとリーダライタとの相互認証に用いられる認証鍵などの、秘密情報のアップデートを、通常のサービスデータの授受とは異なるモードでのICカードとリーダライタ間の通信によって可能とすることができる。

【0280】本発明の第2の情報処理装置、情報処理方法、および記録媒体に記録されているプログラムによれば、データ記憶装置に対する、データの入出力を制御し、所定のサービスに対応するデータおよびデータ記憶装置との認証処理に用いられる複数の認証鍵の記憶を制御し、記憶された複数の認証鍵からデータ記憶装置との認証処理に用いられる認証鍵を選択し、選択された認証鍵を用いて認証処理を行い、記憶されている複数の認証鍵のうち、第1の認証鍵による認証処理が禁止されている場合、第1の認証鍵と異なる第2の認証鍵を選択するようにしたので、ある認証鍵が第3者に漏洩してしまった場合などに、使用することができなくなった認証鍵以外の他の認証鍵を用いて、認証処理を実行することを可能とすることができる。

【図面の簡単な説明】

【図1】ICカードとリーダライタの通信方式および認証方式について説明するための図である。

【図2】カード発行者、サービス提供者、およびカード保持者の関係について説明するための図である。

【図3】ICカードの構成を示すブロック図である。

【図4】ICカードの構成を示すブロック図である。

【図5】図3および図4の暗号処理部について説明するための図である。

【図6】図3および図4のSRAについて説明するための図である。

【図7】図6のSRAに格納される認証用鍵情報について説明するための図である。

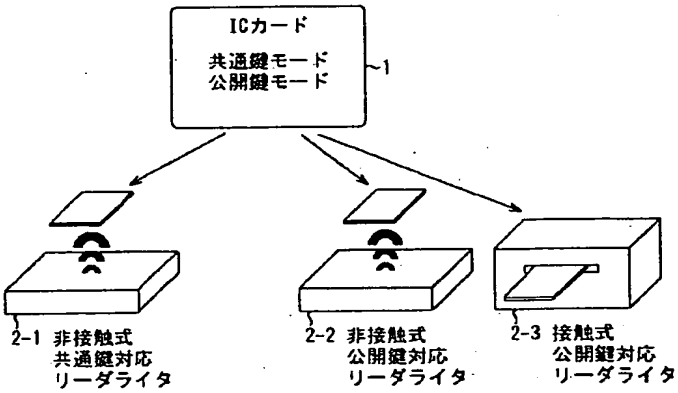
【図8】図3および図4のSRTについて説明するための図である。

【図9】リーダライタの構成を示すブロック図である。

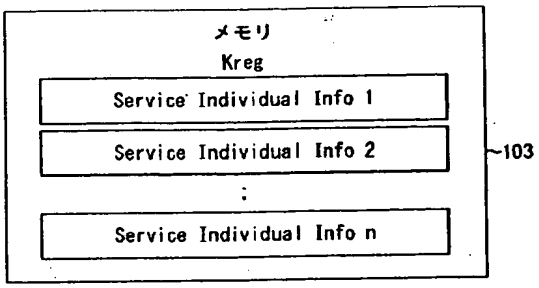
【図10】サービス登録用リーダライタのメモリ情報を説明するための図である。

【図１１】一般リーダライタのメモリ情報を説明するための図である。
【図１２】モジュール間通信用リーダライタのメモリ情報を説明するための図である。
【図１３】モジュール間通信を説明するための図である。
【図１４】バージョンアップ用リーダライタのメモリ情報を説明するための図である。
【図１５】ＩＣカードとリーダライタの認証処理について説明するためのフローチャートである。
【図１６】リーダライタのサービス識別処理について説明するためのフローチャートである。
【図１７】ＩＣカードのサービス識別処理について説明するためのフローチャートである。
【図１８】リーダライタのサービス識別処理について説明するためのフローチャートである。
【図１９】ＩＣカードのサービス識別処理について説明するためのフローチャートである。
【図２０】リーダライタの認証鍵識別処理について説明するためのフローチャートである。
【図２１】ＩＣカードの認証鍵識別処理について説明するためのフローチャートである。
【図２２】リーダライタの認証鍵識別処理について説明するためのフローチャートである。
【図２３】ＩＣカードの認証鍵識別処理について説明するためのフローチャートである。
【図２４】証明書について説明するための図である。
【図２５】署名生成処理について説明するためのフローチャートである。
【図２６】署名検証処理について説明するためのフローチャートである。
【図２７】リーダライタの認証鍵識別処理について説明するためのフローチャートである。
【図２８】ＩＣカードの認証鍵識別処理について説明するためのフローチャートである。
【図２９】サービス登録用リーダライタのサービス登録処理について説明するためのフローチャートである。
【図３０】ＩＣカードのサービス登録処理について説明するためのフローチャートである。
【図３１】サービス登録用リーダライタのサービス削除処理について説明するためのフローチャートである。
【図３２】ＩＣカードのサービス削除処理について説明するためのフローチャートである。
【図３３】一般リーダライタのサービス削除処理について説明するためのフローチャートである。
【図３４】ＩＣカードのサービス削除処理について説明するためのフローチャートである。
【図３５】一般リーダライタのサービスデータ取得処理について説明するためのフローチャートである。
【図３６】ＩＣカードのサービスデータ送信処理について説明するためのフローチャートである。
【図３７】一般リーダライタのサービスデータ取得処理について説明するためのフローチャートである。
【図３８】ＩＣカードのサービスデータ送信処理について説明するためのフローチャートである。
【図３９】一般リーダライタのサービスデータ書き込み処理について説明するためのフローチャートである。
【図４０】ＩＣカードのサービスデータ書き込み処理について説明するためのフローチャートである。
【図４１】一般リーダライタのサービスデータ書き込み処理について説明するためのフローチャートである。
【図４２】ＩＣカードのサービスデータ書き込み処理について説明するためのフローチャートである。
【図４３】バージョンアップ用リーダライタの鍵バージョンアップ処理について説明するためのフローチャートである。
【図４４】ＩＣカードの鍵バージョンアップ処理について説明するためのフローチャートである。
【図４５】一般リーダライタの鍵バージョンアップ処理について説明するためのフローチャートである。
【図４６】ＩＣカードの鍵バージョンアップ処理について説明するためのフローチャートである。
【図４７】ＩＣカードの鍵バージョンアップ処理について説明するためのフローチャートである。
【図４８】モジュール間通信処理について説明するためのフローチャートである。
【図４９】モジュール間通信処理について説明するためのフローチャートである。
【図５０】モジュール間通信処理について説明するためのフローチャートである。
【図５１】モジュール間通信処理について説明するためのフローチャートである。
【符号の説明】
１　ＩＣカード１　リーダライタ、　２１　通信部、　３１　制御部、　３２メモリ、　３３　暗号処理部、　４１　公開鍵処理部、　４２　共通鍵処理部、　４３　その他の暗号処理部、　４５　ＳＲＴ、　４６　ＳＲＡ、　５１　通信部、　５２　共通鍵サービス処理部、　５３　通信部、　５４　公開鍵サービス処理部、　６１　制御部、　６２　メモリ、６３　暗号処理部、　９１　通信部、　１０１　制御部、　１０２　暗号処理部、　１０３　メモリ、　１１１公開鍵処理部、　１１２　共通鍵処理部、　１１３　その他の暗号処理部、　１０５　表示部、　１０６　入力部、　１２１　公開鍵モジュール、　１２２　共通鍵モジュール

【図１】

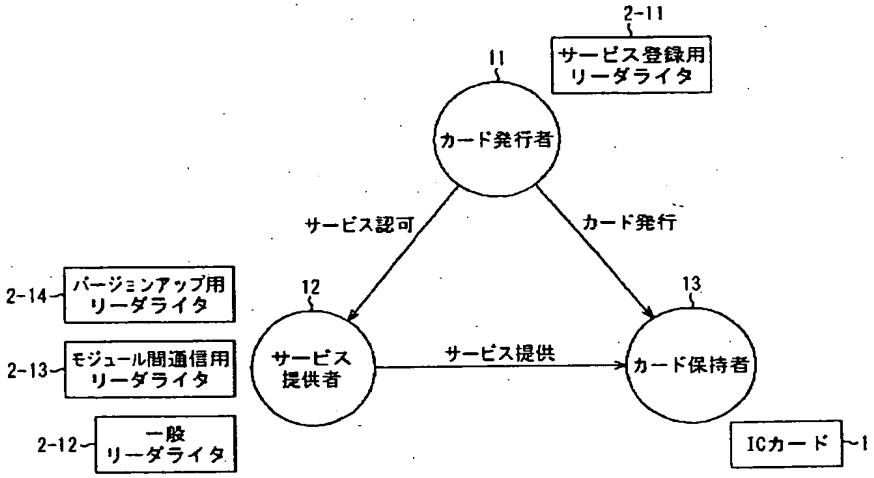


【図１０】

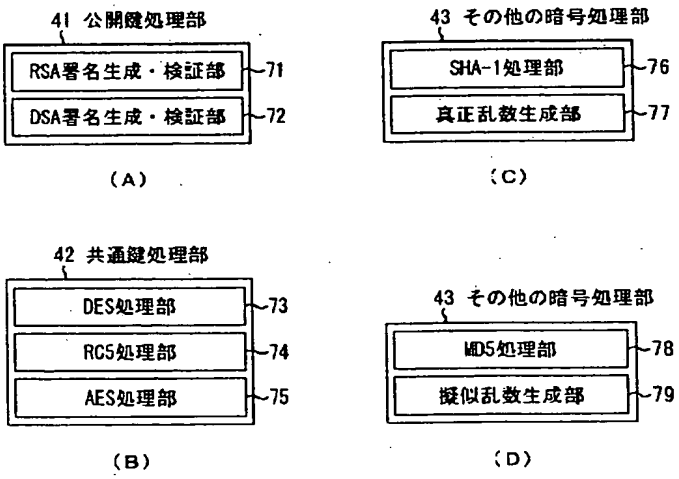


サービス登録用リーダライタ2-11のメモリ情報

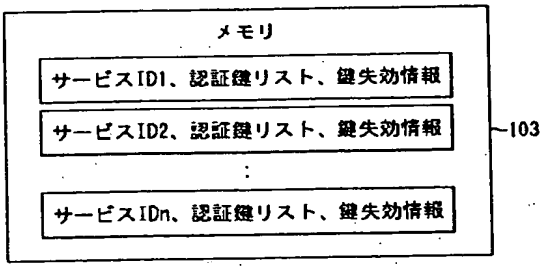
【図２】



【図５】

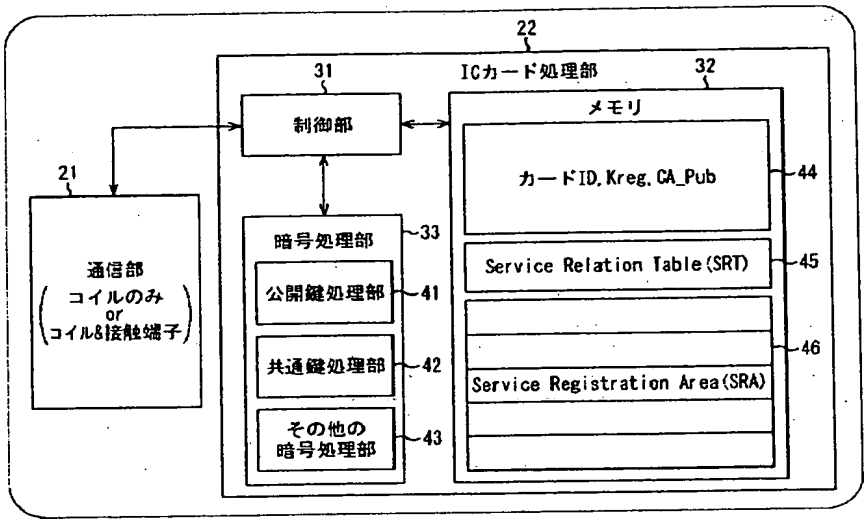


【図１１】



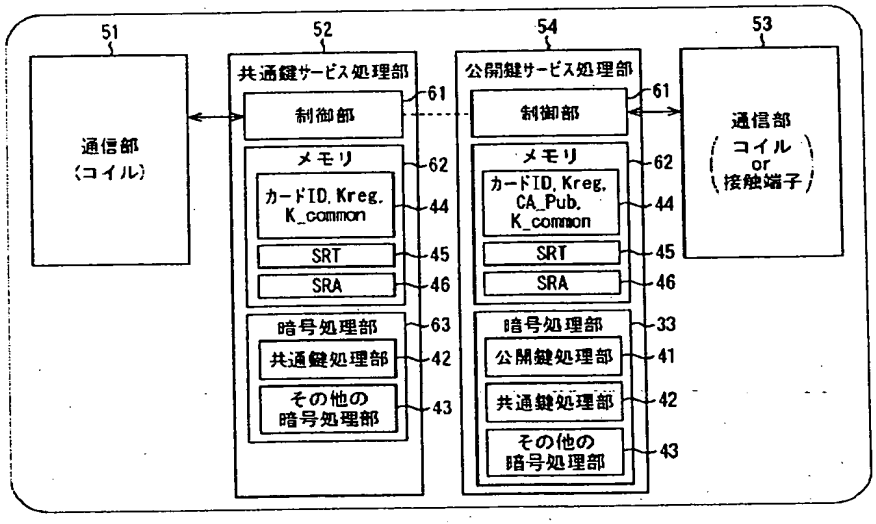
一般リーダライタ2-12のメモリ情報

【図3】



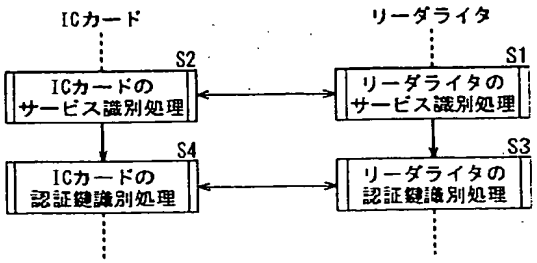
ICカード 1

【図4】

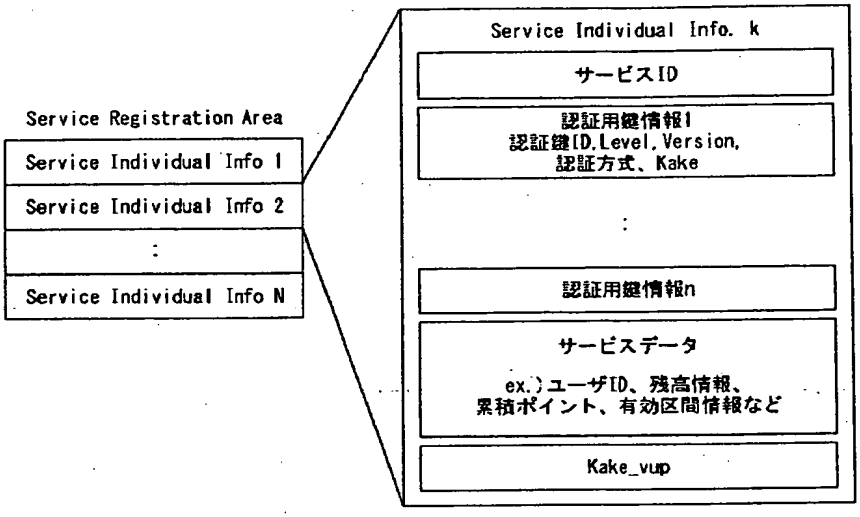


ICカード 1

【図15】



【図6】



SRAに格納されている情報

【図7】

共通鍵・公開鍵の2種類の認証鍵格納状態

(A)

領域No.	認証鍵ID	Version	認証方式	Kake	Certif cate
1	0005	3	共、DES56bit	0100...01	None
2	0018	2	公、ECC128bit	0110...11	証明書データ

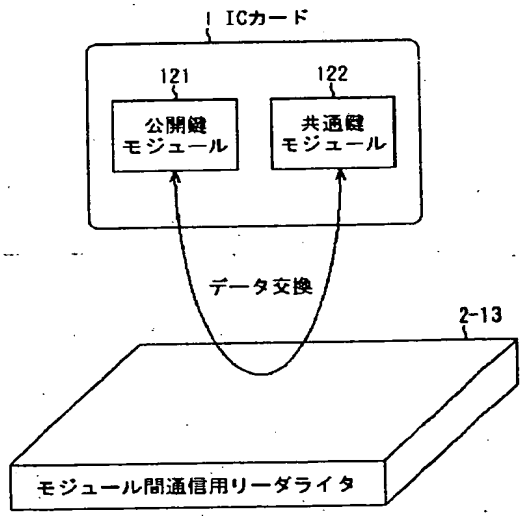
複数レベルの鍵格納状態

(B)

領域No.	認証鍵ID	Level	Version	認証方式	Kake	Certif cate
1	0005	1	3	共、DES56bit	0100...01	None
2	0018	5	2	共、AES128bit	0110...11	None
3	0434	3	1	公、RSA512bit	0011...10	証明書データ
4	0124	6	6	公、RSA2048bit	1011...01	証明書データ
5	0655	2	4	共、AES256bit	1001...00	None
6	0435	4	1	公、ECC160bit	1110...11	証明書データ
7	0342	7	1	公、ECC224bit	0101...10	証明書データ

認証用鍵情報

【図13】



モジュール間通信

【図8】

Service Relation Table

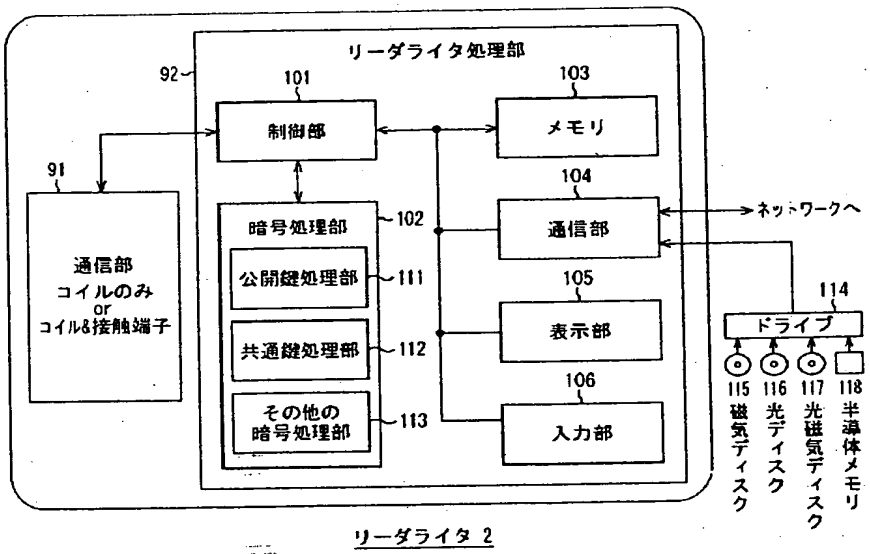
登録サービスID	パーミッション情報
A	
B	C(rw, vup), D(ro)
C	
D	E(rw, vup)
E	A(ro), B(ro), C(ro)
F	G(ro, vup), H(rw, vup)
G	H(rw, vup)
H	
I	B(rw)
J	

ICカード
サービスID
A, B, C, D, E
F, G, H, I, Jに対応

RW:Read and Write allowed
RO:Read Only
VUP:Key Version Up allowed

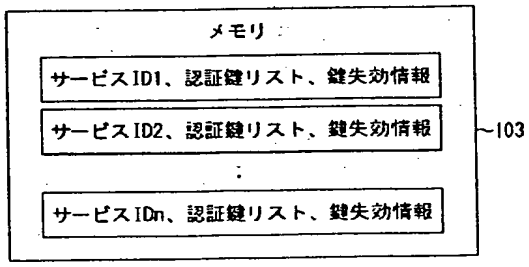
Service Relation Tableに格納されている情報

【図9】



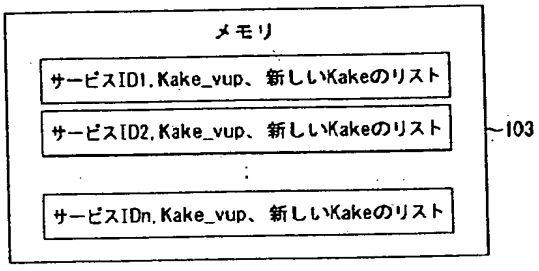
リーダライタ 2

【図12】



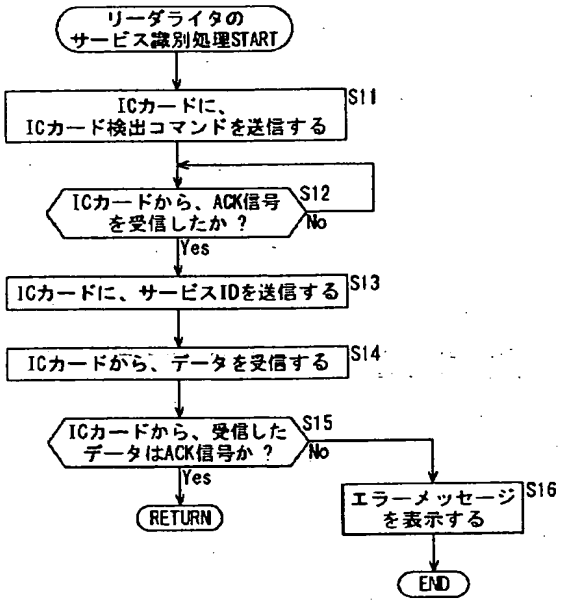
モジュール間通信用リーダライタ 2-13のメモリ情報

【図14】

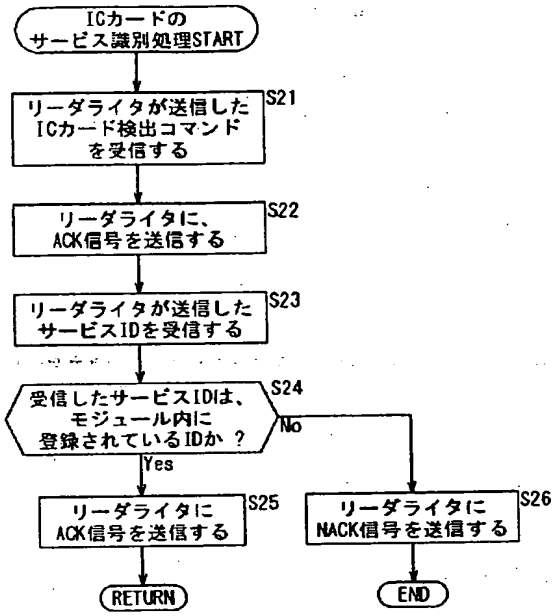


バージョンアップ用リーダライタ 2-14のメモリ情報

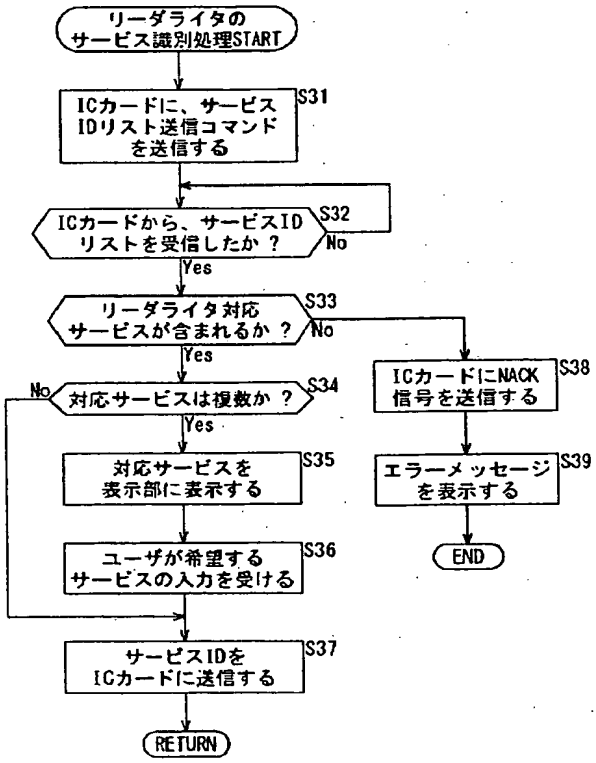
【図16】



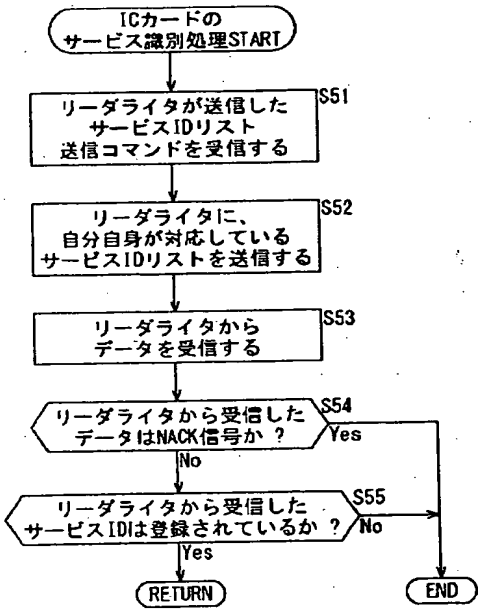
【図17】



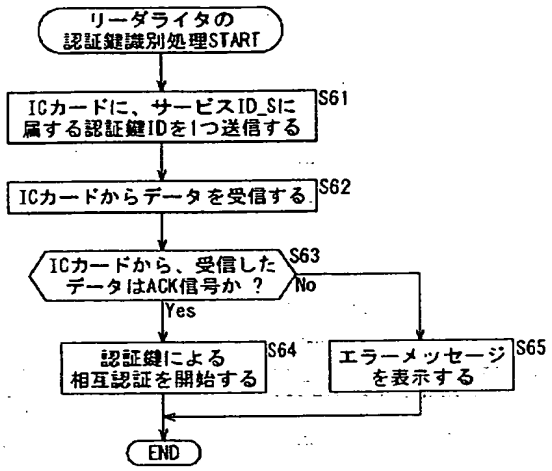
【図18】



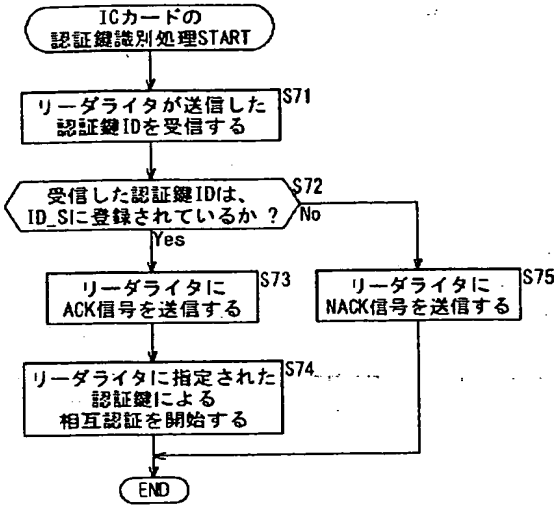
【図19】



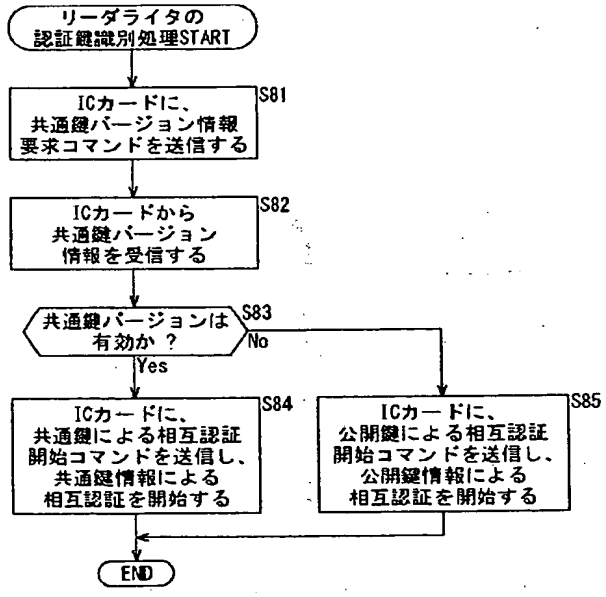
【図20】



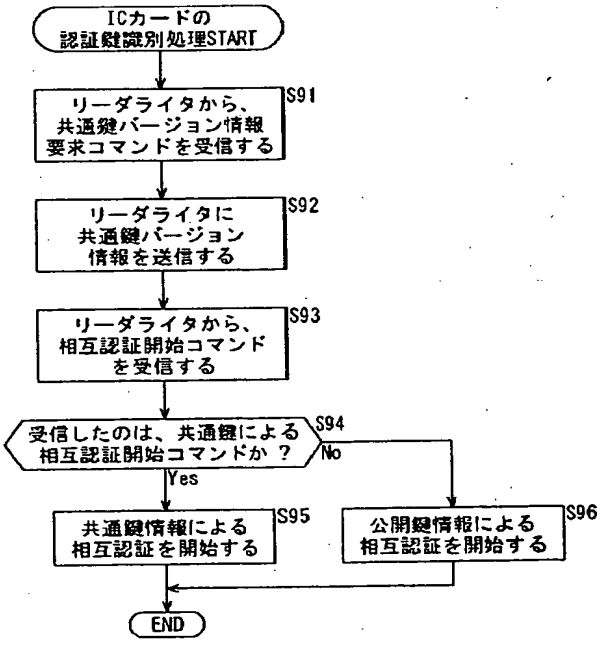
【図21】



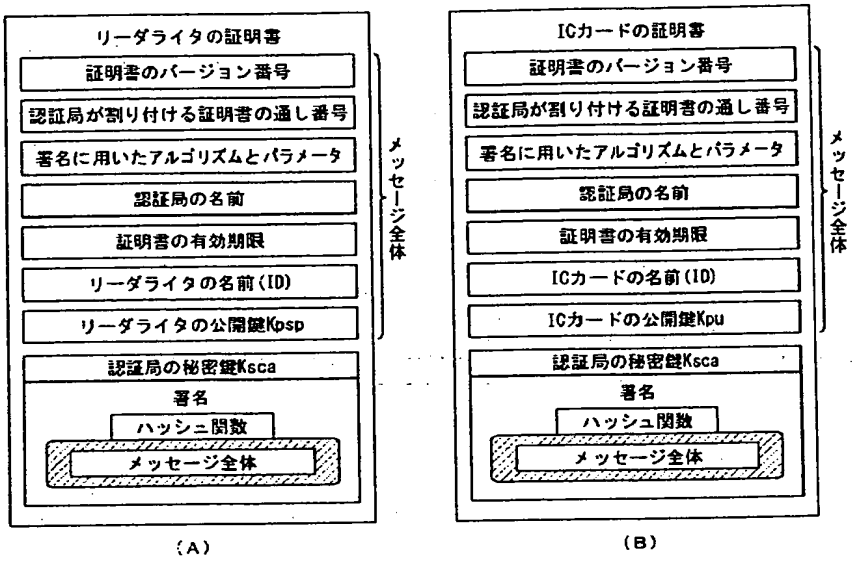
【図22】



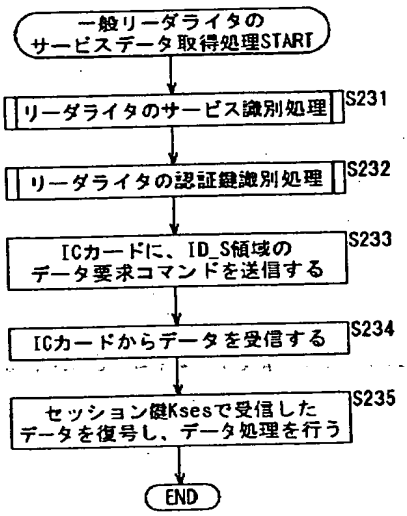
【図23】



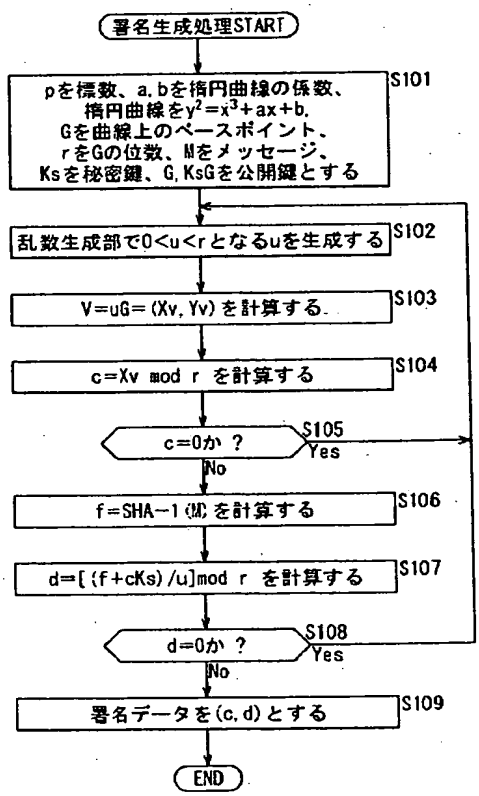
【図24】



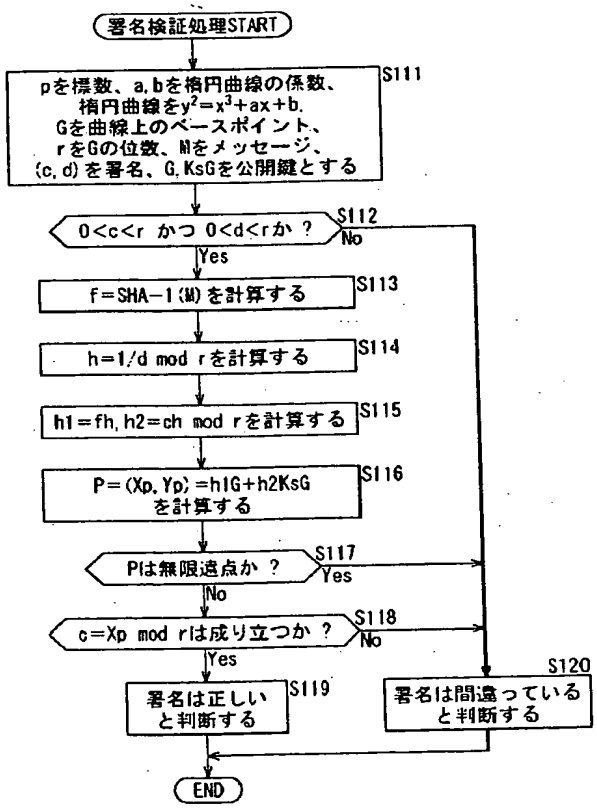
【図35】



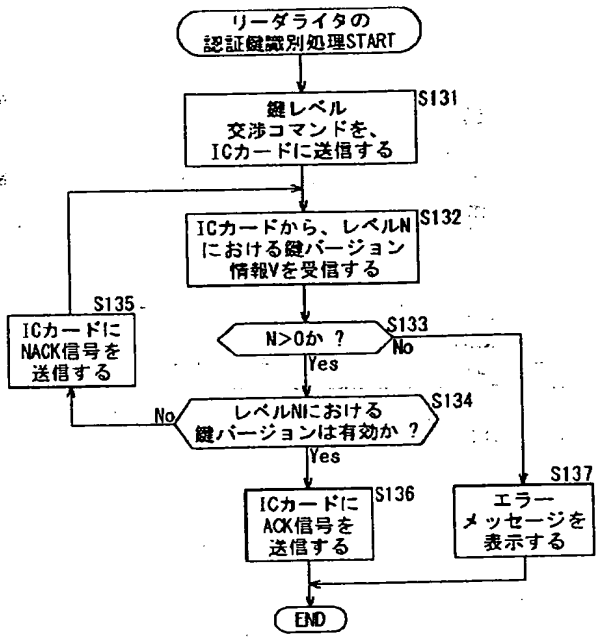
【図25】



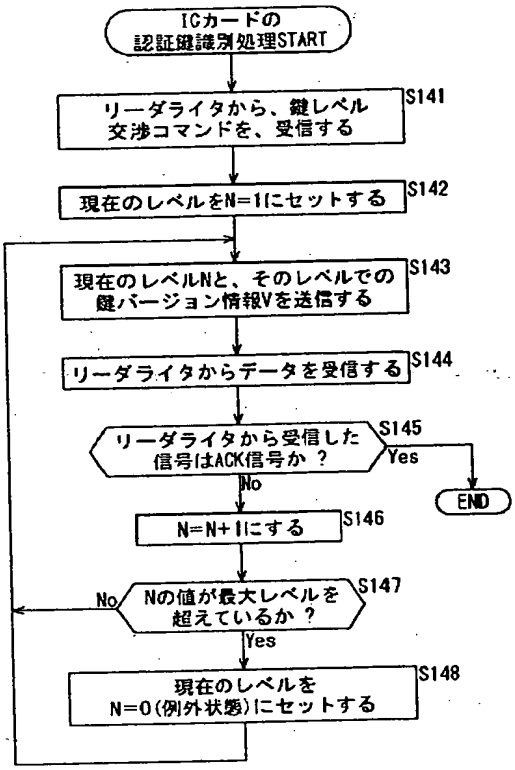
【図26】



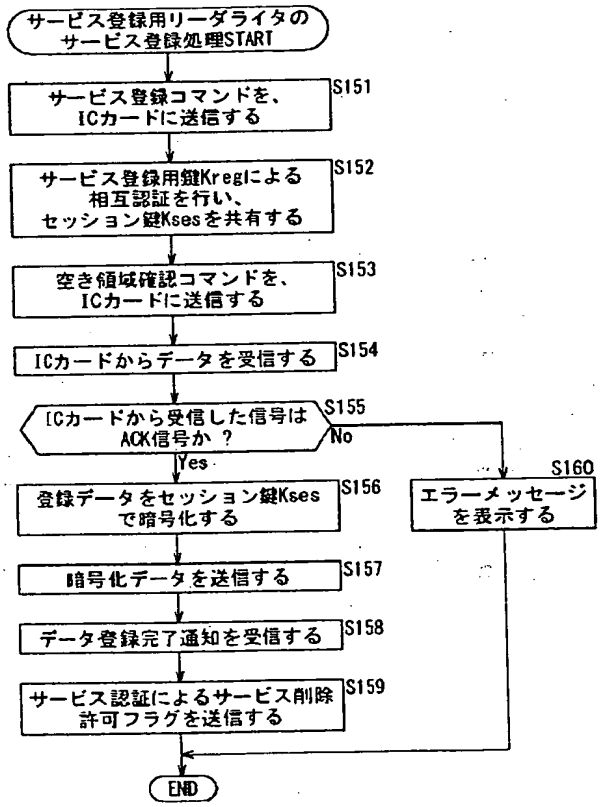
【図27】



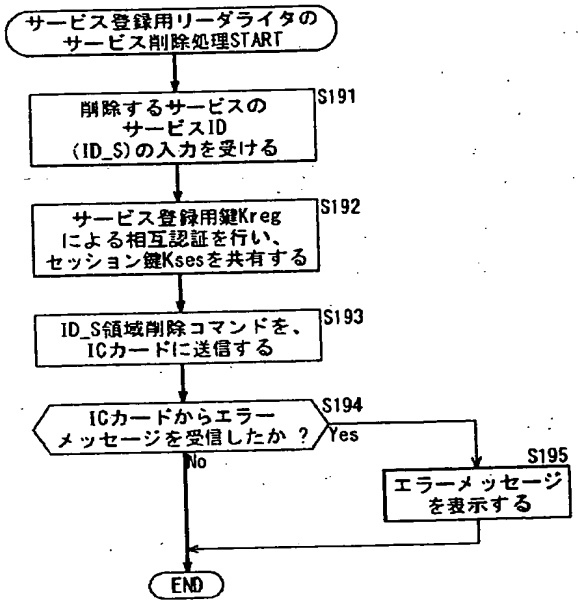
【図28】



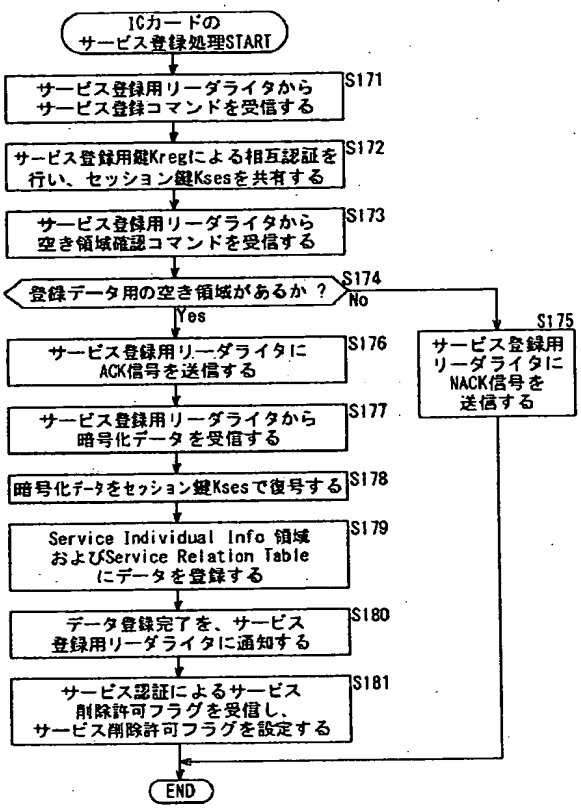
【図29】



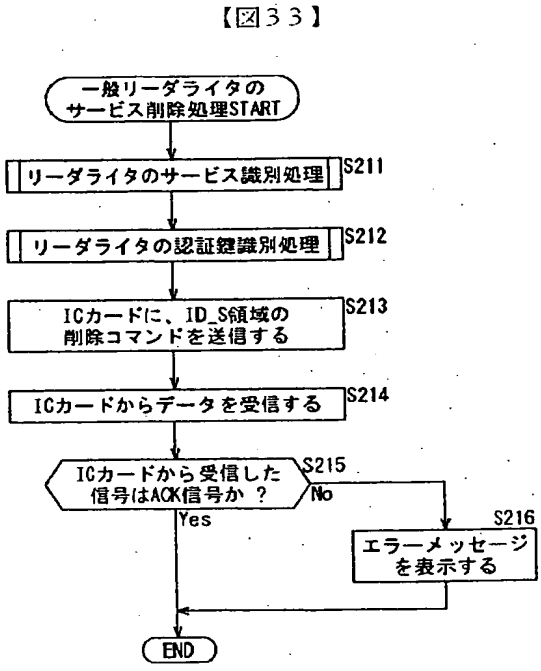
【図31】



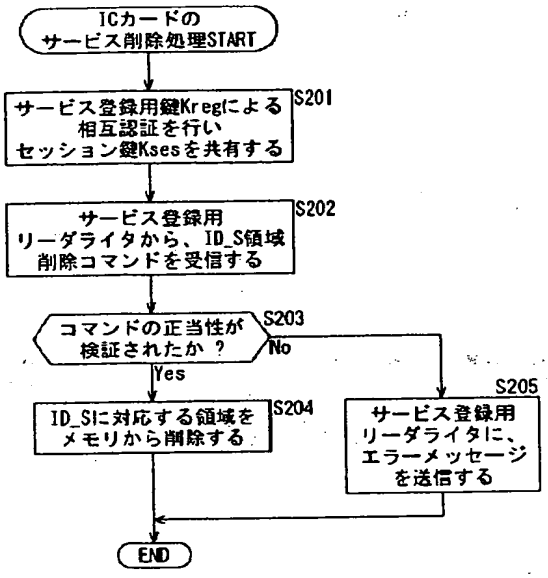
【図30】



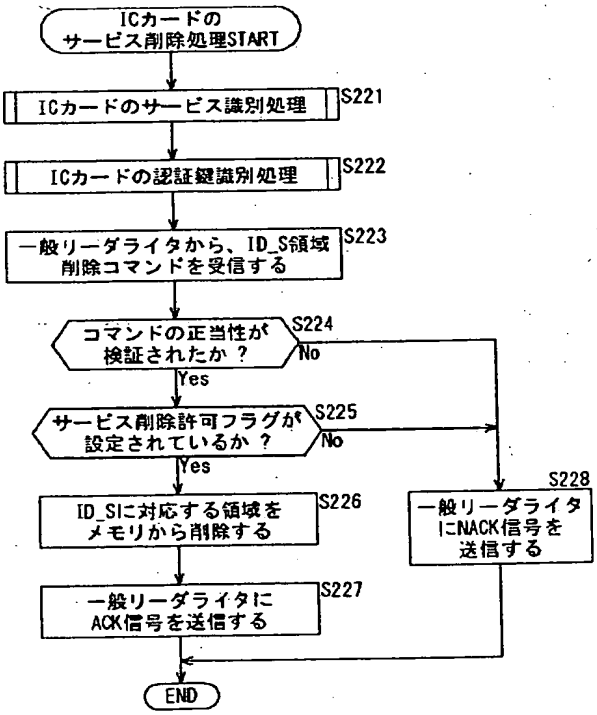
【図31】



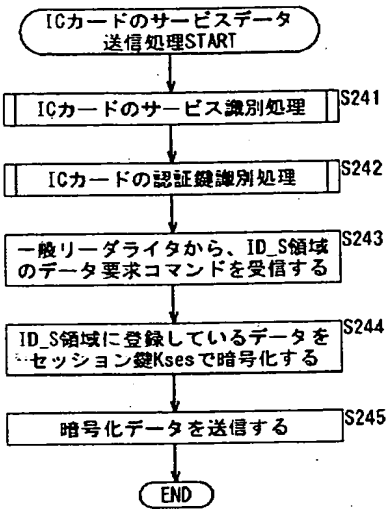
【図32】



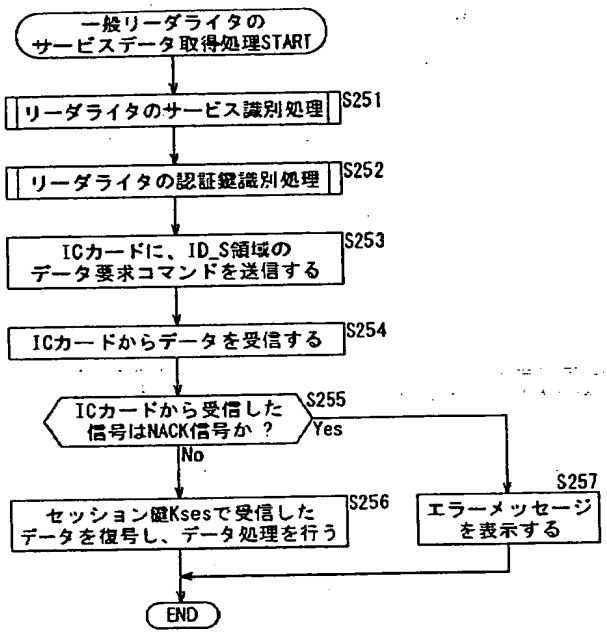
【図34】



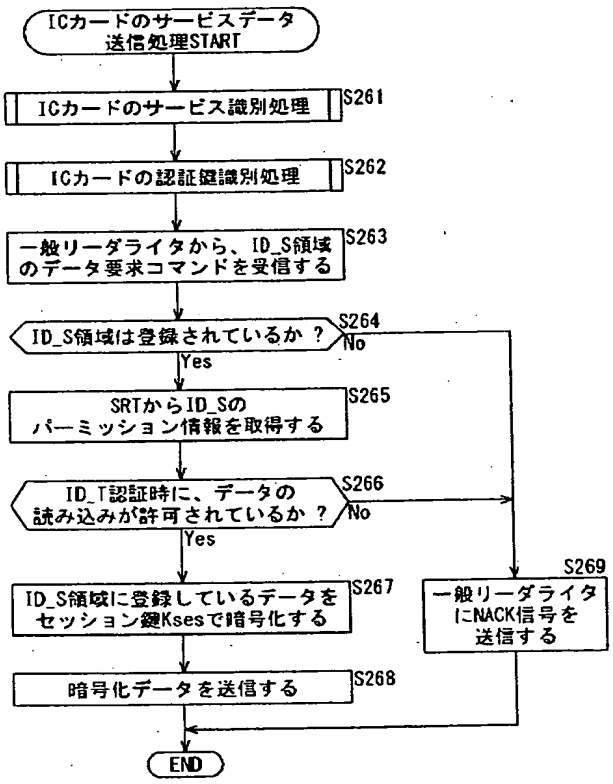
【図36】



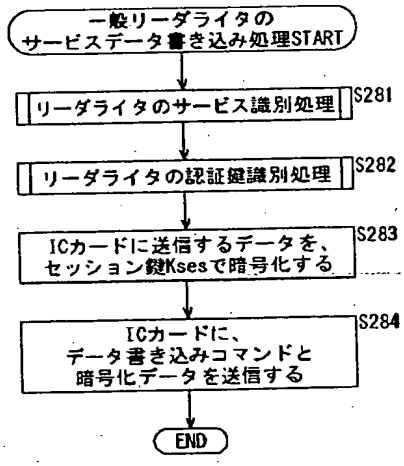
【図37】



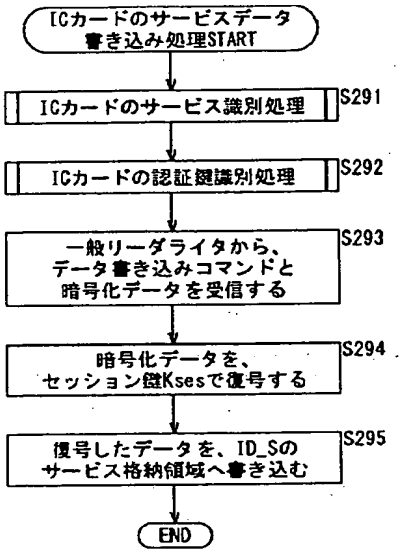
【図38】



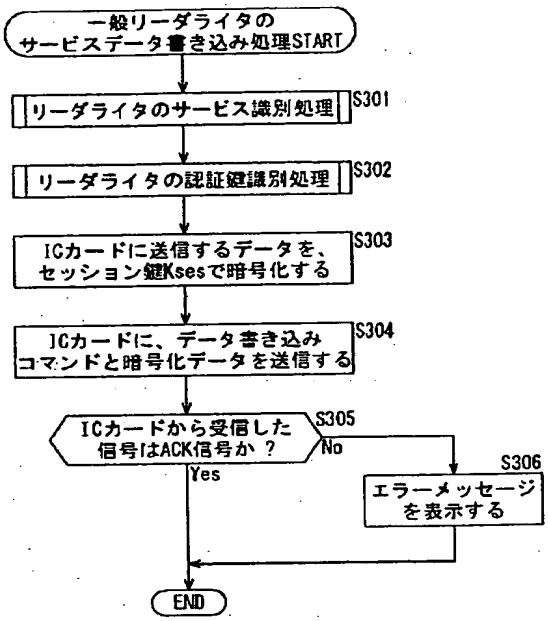
【図39】



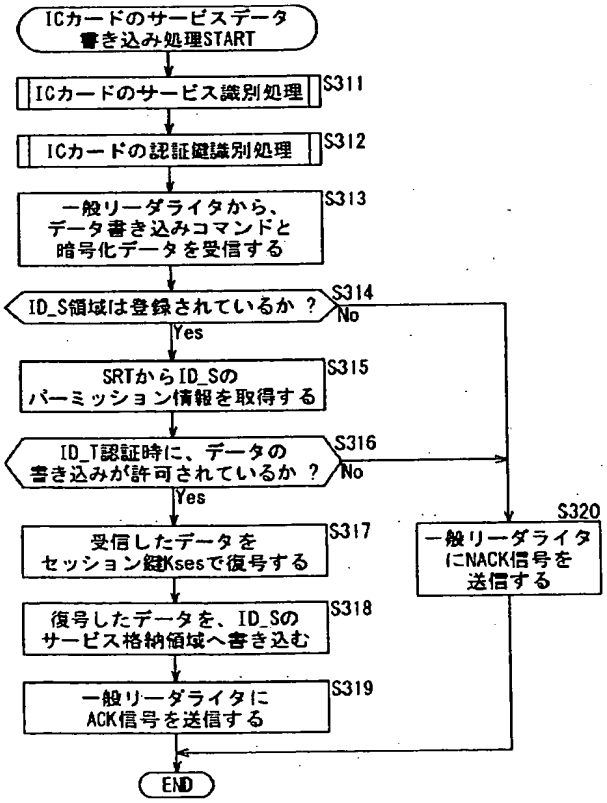
【図40】



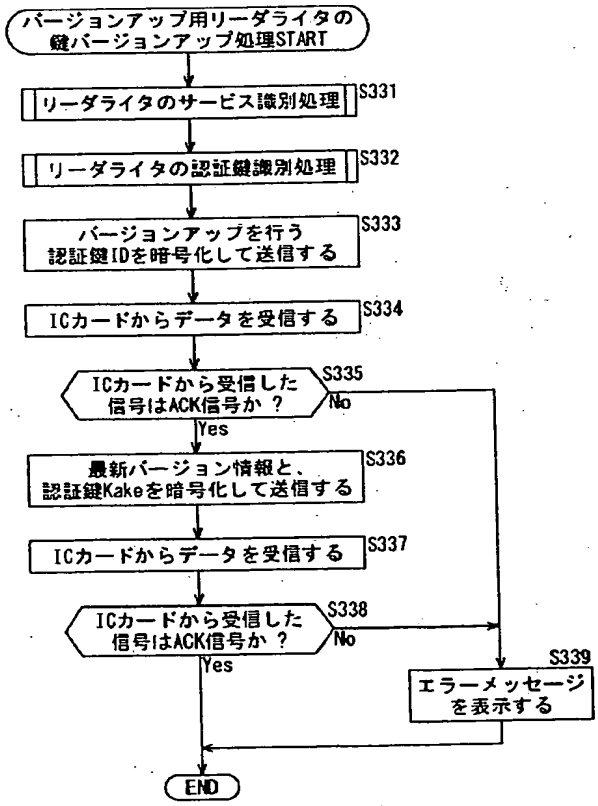
【図41】



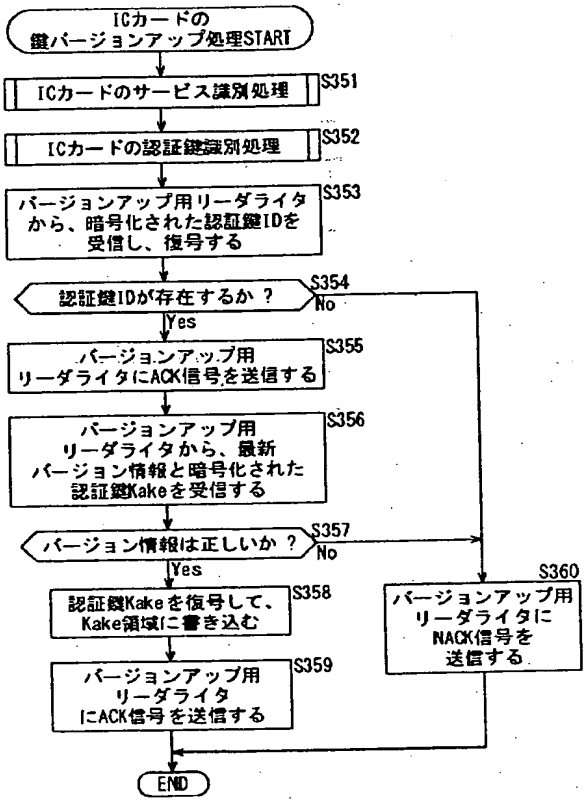
【図42】



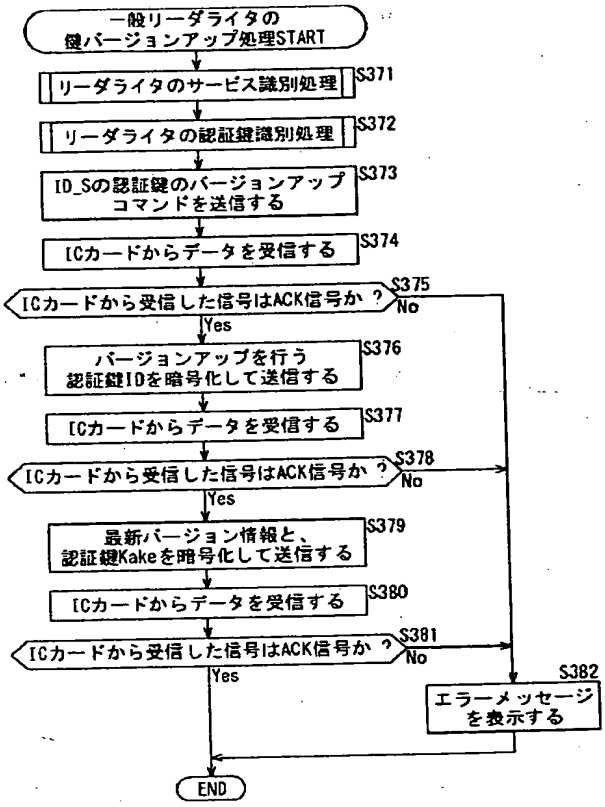
【図43】



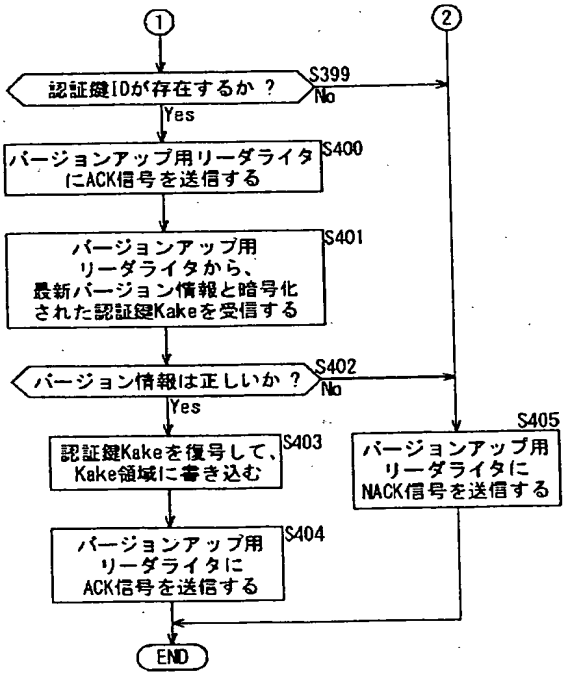
【図44】


ICカードの
鍵バージョンアップ処理START
ICカードのサービス識別処理
S351
ICカードの認証鍵識別処理
S352
バージョンアップ用リーダライタから、暗号化された認証鍵IDを受信し、復号する
S353
認証鍵IDが存在するか？
S354
No
Yes
バージョンアップ用リーダライタにACK信号を送信する
S355
バージョンアップ用リーダライタから、最新バージョン情報と暗号化された認証鍵Kakeを受信する
S356
バージョン情報は正しいか？
S357
No
Yes
認証鍵Kakeを復号して、Kake領域に書き込む
S358
バージョンアップ用リーダライタにACK信号を送信する
S359
バージョンアップ用リーダライタにNACK信号を送信する
S360
END

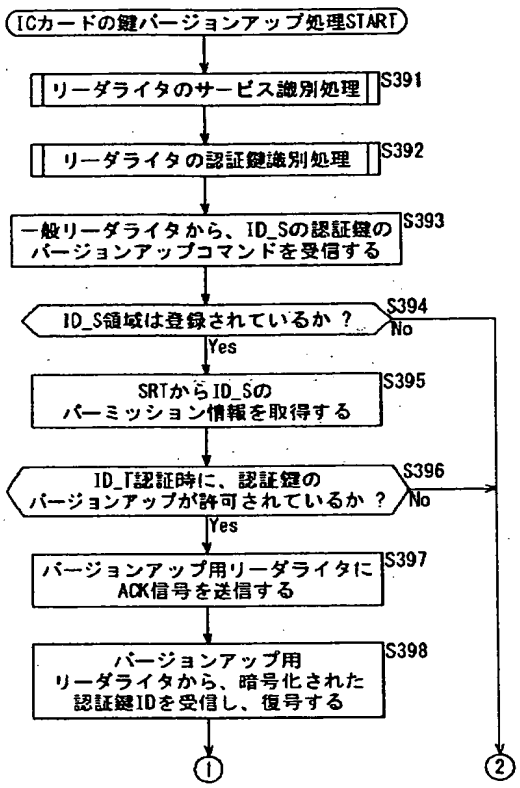
【図45】


一般リーダライタの
鍵バージョンアップ処理START
リーダライタのサービス識別処理
S371
リーダライタの認証鍵識別処理
S372
ID_Sの認証鍵のバージョンアップコマンドを送信する
S373
ICカードからデータを受信する
S374
ICカードから受信した信号はACK信号か？
S375
No
Yes
バージョンアップを行う認証鍵IDを暗号化して送信する
S376
ICカードからデータを受信する
S377
ICカードから受信した信号はACK信号か？
S378
No
Yes
最新バージョン情報と、認証鍵Kakeを暗号化して送信する
S379
ICカードからデータを受信する
S380
ICカードから受信した信号はACK信号か？
S381
No
Yes
エラーメッセージを表示する
S382
END

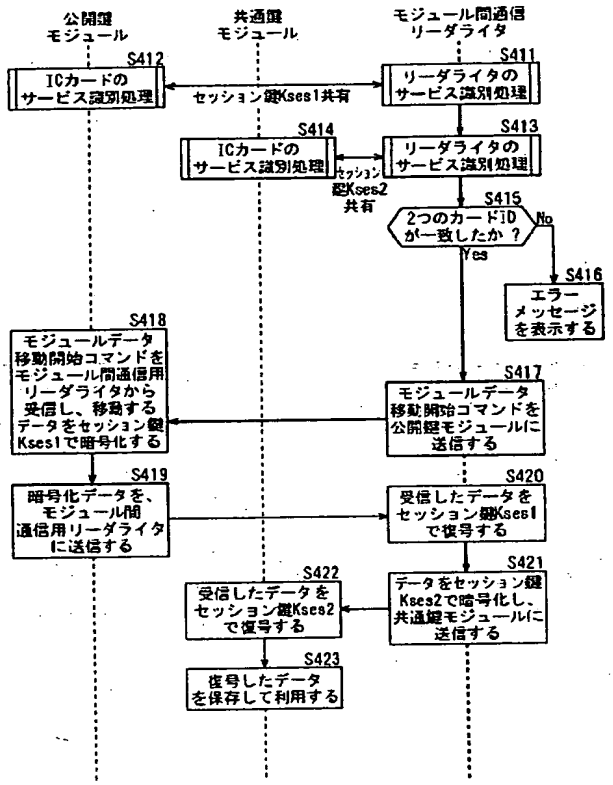
【図47】


①
②
認証鍵IDが存在するか？
S399
No
Yes
バージョンアップ用リーダライタにACK信号を送信する
S400
バージョンアップ用リーダライタから、最新バージョン情報と暗号化された認証鍵Kakeを受信する
S401
バージョン情報は正しいか？
S402
No
Yes
認証鍵Kakeを復号して、Kake領域に書き込む
S403
バージョンアップ用リーダライタにACK信号を送信する
S404
バージョンアップ用リーダライタにNACK信号を送信する
S405
END

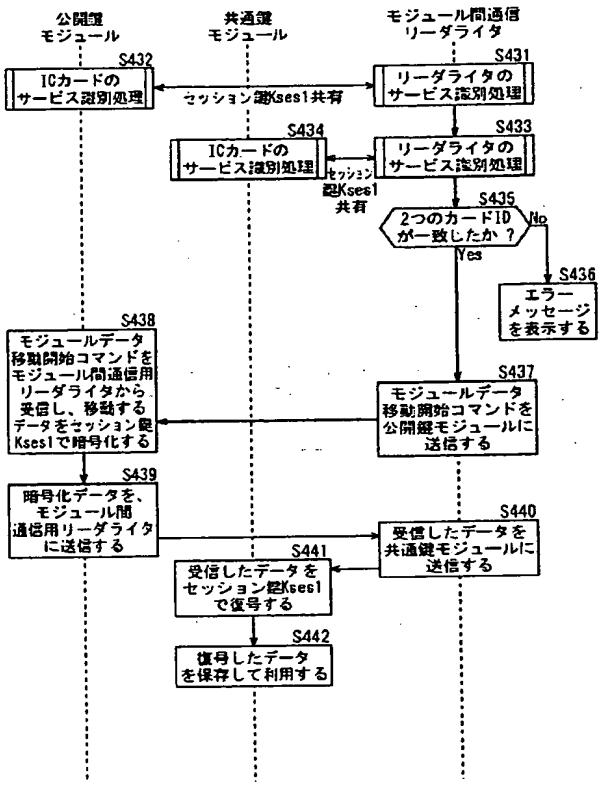
【図46】


ICカードの鍵バージョンアップ処理START
リーダライタのサービス識別処理
S391
リーダライタの認証鍵識別処理
S392
一般リーダライタから、ID_Sの認証鍵のバージョンアップコマンドを受信する
S393
ID_S領域は登録されているか？
S394
No
Yes
SRTからID_Sのパーミッション情報を取得する
S395
ID_T認証時に、認証鍵のバージョンアップが許可されているか？
S396
No
Yes
バージョンアップ用リーダライタにACK信号を送信する
S397
バージョンアップ用リーダライタから、暗号化された認証鍵IDを受信し、復号する
S398
①
②

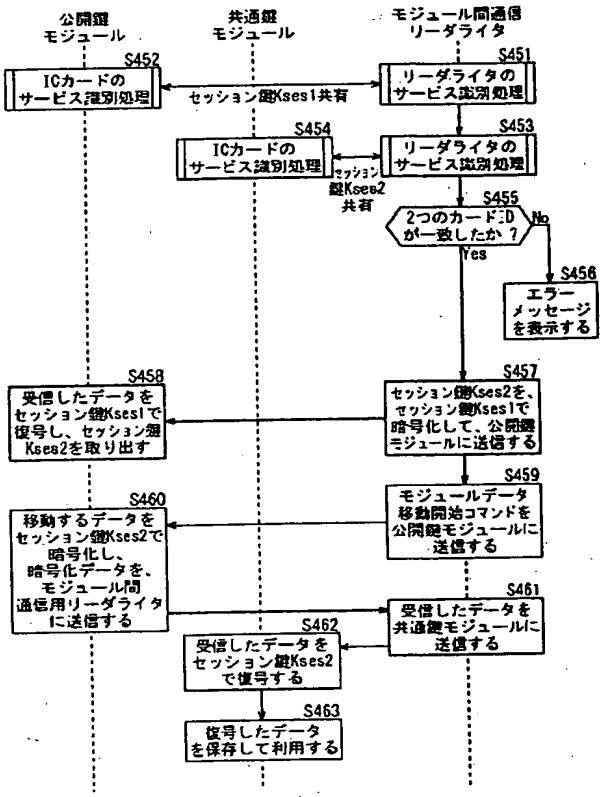
【図48】


公開鍵モジュール
共通鍵モジュール
モジュール間通信リーダライタ
S412
ICカードのサービス識別処理
セッション鍵Kses1共有
S411
リーダライタのサービス識別処理
S414
ICカードのサービス識別処理
セッション鍵Kses2共有
S413
リーダライタのサービス識別処理
S415
2つのカードIDが一致したか？
No
Yes
S416
エラーメッセージを表示する
S418
モジュールデータ移動開始コマンドをモジュール間通信用リーダライタから受信し、移動するデータをセッション鍵Kses1で暗号化する
S417
モジュールデータ移動開始コマンドを公開鍵モジュールに送信する
S419
暗号化データを、モジュール間通信用リーダライタに送信する
S420
受信したデータをセッション鍵Kses1で復号する
S422
受信したデータをセッション鍵Kses2で復号する
S421
データをセッション鍵Kses2で暗号化し、共通鍵モジュールに送信する
S423
復号したデータを保存して利用する

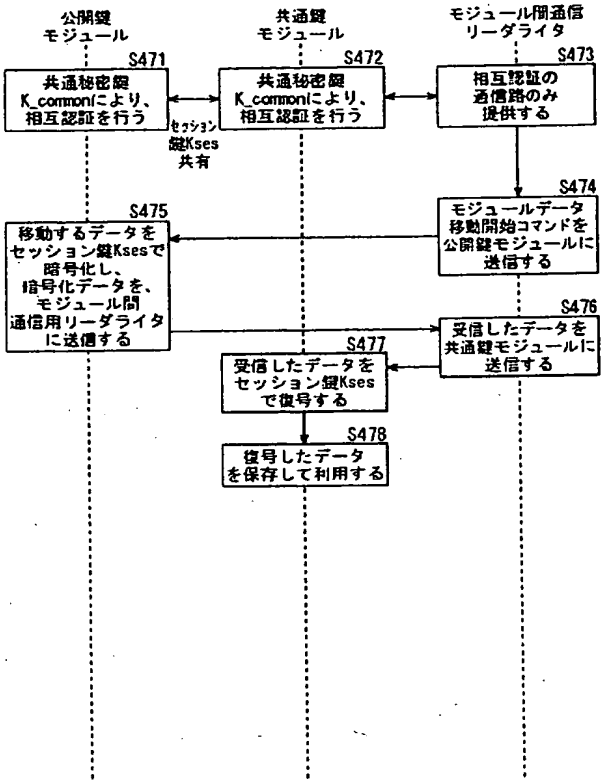
【図49】


公開鍵モジュール
共通鍵モジュール
モジュール間通信リーダライタ
S432
ICカードのサービス識別処理
セッション鍵Kses1共有
S431
リーダライタのサービス識別処理
S434
ICカードのサービス識別処理
セッション鍵Kses1共有
S433
リーダライタのサービス識別処理
S435
2つのカードIDが一致したか？
No
Yes
S436
エラーメッセージを表示する
S438
モジュールデータ移動開始コマンドをモジュール間通信用リーダライタから受信し、移動するデータをセッション鍵Kses1で暗号化する
S437
モジュールデータ移動開始コマンドを公開鍵モジュールに送信する
S439
暗号化データを、モジュール間通信用リーダライタに送信する
S440
受信したデータを共通鍵モジュールに送信する
S441
受信したデータをセッション鍵Kses1で復号する
S442
復号したデータを保存して利用する

【図50】


公開鍵モジュール
共通鍵モジュール
モジュール間通信リーダライタ
S452
ICカードのサービス識別処理
セッション鍵Kses1共有
S451
リーダライタのサービス識別処理
S454
ICカードのサービス識別処理
セッション鍵Kses2共有
S453
リーダライタのサービス識別処理
S455
2つのカードIDが一致したか？
No
Yes
S456
エラーメッセージを表示する
S458
受信したデータをセッション鍵Kses1で復号し、セッション鍵Kses2を取り出す
S457
セッション鍵Kses2を、セッション鍵Kses1で暗号化して、公開鍵モジュールに送信する
S459
モジュールデータ移動開始コマンドを公開鍵モジュールに送信する
S460
移動するデータをセッション鍵Kses2で暗号化し、暗号化データを、モジュール間通信用リーダライタに送信する
S461
受信したデータを共通鍵モジュールに送信する
S462
受信したデータをセッション鍵Kses2で復号する
S463
復号したデータを保存して利用する

【図51】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	テーマコード(参考)
H04L 9/10		H04L 9/00	621A
9/32			673E

(72)発明者 浅野 智之
東京都品川区北品川6丁目7番35号 ソニー株式会社内
(72)発明者 吉野 賢治
東京都品川区北品川6丁目7番35号 ソニー株式会社内
(72)発明者 白井 太三
東京都品川区北品川6丁目7番35号 ソニー株式会社内
(72)発明者 瀧 隆太
東京都品川区北品川6丁目7番35号 ソニー株式会社内

Fターム(参考) 5B035 AA13 BB09 BC00 CA23 CA38
5B058 CA13 CA15 CA27 KA02 KA04
KA08 KA35 YA20
5J104 AA07 AA16 EA17 KA01 NA02
NA03 NA12 NA35 NA36 NA37
NA38 NA40